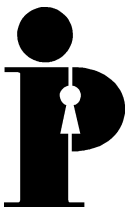
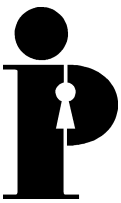
Information
and Privacy
Commissioner/
Ontario

Consumer Biometric Applications:

A Discussion Paper



Ann Cavoukian, Ph.D.
Commissioner
September 1999



Information and Privacy Commissioner/Ontario

2 Bloor Street East
Suite 1400
Toronto, Ontario
M4W 1A8

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

This publication is also available on the IPC website.

Cette publication est également disponible en français.

Table of Contents

Introduction

Biometrics: Identifying human beings has become a multibillion dollar industry[1]

From Sci-Fi to Security: Biometrics move beyond Star Trek into reality[2]

The eyes have it: Bank machines to use iris scans?[3]

Computers that recognize your smile[4]

Human identity reduced to a bar code[5]

Big Brother biometrics: the identification you'll never leave home without[6]

Increasingly, Canadians are seeing headlines like these in their local newspapers and favourite online news sources. More importantly, in the near future, they most likely will be faced with the use of biometrics as consumers. Their banks, health clubs, hotels, automobiles, and personal computers are going to start using this technology to identify them.

The Office of the Information and Privacy Commissioner/Ontario (IPC) has a mandate under the *Freedom of Information and Protection of Privacy Act* and the *Municipal Freedom of Information and Protection of Privacy Act* to research and comment on issues relating to the protection of privacy, and to educate the public about such matters. The IPC has been following the development of biometric technology and is concerned that, if not carefully implemented and managed, it could represent a significant threat to consumer privacy.

In an effort to ensure that the introduction of biometrics in the commercial environment does not unduly compromise privacy, and that Canadian consumers are in a position to make informed choices, this paper provides an overview of the technology, as well as outlines a number of issues and concerns consumers should consider prior to consenting to the use of their biometric data.

Definition

In the context of this discussion, biometrics are techniques that analyze human characteristics to distinguish one person from another — even identical twins. A more formal definition is:

> A biometric is a unique, measurable characteristic or trait of a human being for automatically recognizing or verifying identity.[7]

This definition contains several important components critical to biometrics:

- **Unique:** In order for something to be unique, it has to be the one and only, have no like or equal, and be different from all others.[8] When trying to identify an individual with certainty, finding something that is unique to that person is absolutely essential.
- **Measurable:** In order for identification to be reliable, the item being used must be relatively static and easily quantifiable. For example, hair style or colour are not dependable characteristics for identifying an individual, as both can be easily and frequently changed.
- **Characteristic or Trait:** Today, identity is often confirmed by something a person *has*, such as a card or token (e.g., a drivers license), or something they *know*, such as their computer password or their personal identification number (PIN) for their bank machine.[9]

  Biometrics involve something a person *is or does*. These types of characteristics or traits are intrinsic to a person and can be divided into physiological (i.e., something a person *is*) such as their fingerprints, voiceprints, or patterns in their eyes, and behavioural (i.e., something a person *does*), such as the way they sign their name or type on a keyboard.
- **Automatic:** In order for something to be automatic it must work by itself, without direct human intervention.[10] For a process to be considered a biometric technology, it must recognize or verify a human characteristic quickly (e.g., some biometric systems function in under two seconds) and without a high level of human involvement.[11]
- **Recognition:** To recognize someone is to identify them as someone who is known, or to "know again."[12] A person cannot recognize someone who is completely unknown to them. A computer system can be designed to recognize or identify a person based on a biometric characteristic. To do this it must compare a biometric presented by a live person against all biometric samples stored in a central database. If the presented biometric matches a sample on file, the system then identifies the individual. This is often called a one-to-many match. Essentially, the system is trying to answer the question: Who is this person?

- **Verification:** To verify something is to establish its truth or correctness.[13] To do this in terms of identity, a computer system can be designed to compare a biometric presented by a person against a stored sample previously given by that individual and identified as such. If the two samples match, the system confirms or authenticates the individual as the owner of the biometric on file. This is called a one-to-one match, and the biometric can be stored in a central database or on a card or token. Here the system is trying to answer the question: Is this person who they say they are?

- **Identity:** This term can be defined as the condition of "being a specific person" or "being oneself." It implies a state of being or quality that defines one's self.[14] It is important to distinguish between "identity" and "identification." Identification is the process of associating or linking specific data with a particular person. In the context of this paper, a biometric is considered an identifier; it does not define a person's identity or who they are, rather it links specific data with that person.

The distinction between recognition/identification versus verification/authentication is very important. The difference in purpose, or in the question that the system is trying to answer, greatly influences how the biometric data is used and stored. These issues are paramount in the context of the privacy concerns associated with biometric technology, discussed later in the paper.

The purpose of a verification system is not necessarily to confirm a person's identity, but rather to authenticate that person's eligibility to access a particular service. Essentially, there are three components to authentication:

1. **Identification:** this is a one time process to establish an individual as a unique, named person.

2. **Confirmation of Eligibility:** again, this is a one time process to confirm that the named individual is eligible for the benefit or service to be accessed by the biometric.

3. **Authentication Credential:** this is something that identifies the individual as eligible, and permits them to access the service or benefit on a recurring basis. Traditionally, these credentials have been in the form of cards, passwords or PINs. Now biometrics are being used in this capacity.[15]

Once an individual's identity has been established, and they have demonstrated eligibility for the service in question, from that point on, their biometric serves as their authentication credential. When a one-to-one match is made on the biometric, the existence of the other two components (i.e., identification and confirmation of eligibility) may be presumed, for it could not occur without them. With this process, it is not necessary to identify the individual every time they want to access the service.[16] Identification need only be done once. This process is very different from one-to-many matches where identification is done each and every time a person presents a biometric.

How Biometric Systems Work

While a biometric is the actual characteristic or trait, a biometric system is the computer hardware and software used to recognize or verify an individual. Although it must be acknowledged that there are many variations in how specific products and systems work, there are a number of common processing elements.

Collection

As a first step, a system must collect or "capture" the biometric to be used. One essential difference between the various techniques is the characteristic (i.e., body part or function) being analyzed. Obviously, this will influence the method of capture.

All biometric systems have some sort of collection mechanism. This could be a reader or sensor upon which a person places their finger or hand, a camera that takes a picture of their face or eye, or software that captures the rhythm and speed of their typing.

In order to "enrol" in a system, an individual presents their "live" biometric a number of times so the system can build a composition or profile of their characteristic, allowing for slight variations (e.g., different degrees of pressure when they place their finger on the reader). Depending upon the purpose of the system, enrolment could also involve the collection of other personally identifiable information.

Extraction

Commercially available biometric devices generally do not record full images of biometrics the way law enforcement agencies collect actual fingerprints. Instead, specific features of the biometric are "extracted." Only certain attributes are collected (e.g., particular measurements of a fingerprint or pressure points of a signature). Which parts are used is dependent upon the type of biometric, as well as the design of the proprietary system.

This extracted information, sometimes called "raw data," is converted into a mathematical code. Again, exactly how this is done varies amongst the different proprietary systems. This code is then stored as a "sample" or "template." The specific configuration of a system will dictate what, how, and where that information is stored. Regardless of the variations, all biometric systems must create and retain a template of the biometric in order to recognize or verify the individual.

While the raw data can be translated into a set of numbers for the template, commercial biometric systems are generally designed so that the code cannot be re-engineered or translated back into the extracted data or biometric.

Comparison and Matching

To use a biometric system, the specific features of a person's biometric characteristic are measured and captured each time they present their "live" biometric. This extracted information is translated into a mathematical code using the same method that created the template. The new code created from the live scan is compared against a central database of templates in the case of a one-to-many match, or to a single stored template in the case of a one-to-one match. If it falls within a certain statistical range of values, the match is considered to be valid by the system.[17]

Types of Biometrics

Canadians are most familiar with the use of biometrics in the context of law enforcement. The law enforcement community is the largest biometric user group. Biometric spending in 1998 was 50% law enforcement, 30% financial services, 12% security and 8% other.[18]

Police forces throughout the world use Integrated Automated Fingerprint Identification Systems (IAFIS) or 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.[19]

Around the world, governments at all levels use biometrics for both recognition and verification purposes. In Ontario, a recent example was the City of Toronto's proposed introduction of a encrypted fingerscan as part of its Client Identification and Benefits System to combat a particular type of welfare fraud known as "double-dipping."[20]

Employers also utilize biometrics to help protect the safety and security of their staff and physical assets. In addition, biometrics are used to record the attendance and movement of employees.

These types of applications are not, however, the focus of this paper. Instead, the growing commercial use of biometrics is examined. So far, consumer applications are limited to the verification of identity; many in the context of access control to secure locations, equipment, and information. Biometric technology continues to evolve and expand, with new developments and applications announced regularly. Below is a brief overview of the main categories of biometrics in use today.

Eye

There are two main types of biometric analysis of the eye. One involves the iris, which is the coloured ring that surrounds the pupil, and the other uses the retina, which is the layer of blood vessels at the back of the eye.

Iris

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"[21] 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 not susceptible to wear and injury. Contact lenses do not interfere with the use of this biometric identifier. Iris recognition technology involves the use of a camera to capture a digital image of the eye, from

which data are extracted. This type of biometric technology can be used for one-to-one verification or one-to-many recognition.[22] Examples of iris recognition applications used by consumers are:

- 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.[23]
- Some Automatic Teller Machine (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. Reportedly, several other American banks are expected to unveil iris identification ATMs later in 1999. In addition, the technology already is used by eleven different banks outside of the United States.[24]
- The Royal Bank of Canada and the Canadian Imperial Bank of Commerce recently tested an ATM with iris scanning capabilities in Toronto.[25]

There is very little research into Canadians' attitudes toward biometrics. However, in 1997, one Canadian bank carried out limited customer surveys on the use of biometrics and received an "overwhelmingly negative reaction" to the idea of the use of iris scans.[26]

Retina

As with the iris, the retina forms a unique pattern that begins to decay quickly after death. Unauthorized access to a retinal system is reported to be virtually impossible. With this type of system, a one-to-many identification is usually the comparison performed.

A precise enrolment procedure is necessary. A user must focus on a specific point and then the system uses a beam of light to capture the unique retinal characteristics. The downside of retinal scanning is people's reluctance to have light shone into their eyes to gather information.[27] For this reason, Canadian consumers are not likely to see retinal scans in general use in the near future. Retinal biometrics usually are found in high security applications where inconvenience and user comfort are not important considerations.

Face

There are two main types of facial recognition systems; the most common uses video, while the other uses thermal imaging.

Video face recognition technology analyze the unique shape, pattern and positioning of facial features. A video camera is used to capture an image from a distance of a few feet away from the user. A number of points on the face (e.g., position of the eyes, mouth and nostrils) are usually mapped out. With other systems, a three-dimensional map of the face can be created.

Most systems feature a "face locating" function that searches for faces within the field of view. This permits people of different heights to use the system while standing. Face recognition systems are designed to compensate for expression, glasses, hats and beards.[28]

A facial thermogram uses an infrared camera to scan a person's face and then digitize the thermal patterns.[29] Apparently no two people, not even identical twins, have the same facial thermogram. The patterns are created by the branching of blood vessels in the face. As the blood is hotter than the tissue surrounding it, it radiates heat that can be picked up at a distance. Plastic surgery does not change a thermogram unless it involves the rerouting of the flow of blood. In addition, time does not alter a thermogram.[30] However, it is thought that alcohol consumption can radically change a person's thermogram.[31]

While face recognition is being used in a one-to-many capacity by law enforcement and government, commercial applications use this technology for one-to-one verification. The use of video-based face recognition for consumer applications has grown considerably in the last few years. Some American banks, gas stations and convenience stores are using this technology to identify and record cheque-cashing transactions.[32] One American 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, irrefutable, permanent record of the transaction.[33]

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 authorized, the box is retrieved by robots and delivered to the owner by an automated handling system.[34]

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.[35]

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.

Facial recognition can be done on a more remote basis so a person will not know their face is being analyzed. For example, 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 digitized photo database of "known cheaters."[36] Globally, airports have expressed interest in another system that can pick a moving face out of a crowd.[37] They hope to use this technology as a way of identifying terrorists and other criminals.[38]

Fingerscanning

As previously noted, use of the fingerprint by law enforcement for identification purposes is common place and widely accepted. However, the technology has diversified, migrating away from law enforcement towards civil and commercial markets. In the context of commercial applications, the preferred term is "fingerscanning," which is the process of finger image capture.[39]

There are a number of different types of fingerscanning systems on the market. Some analyze the distinct marks on the finger called "minutiae" points. Others examine the pores on the finger that are uniquely positioned. Finger image density or the distance between ridges also may be analyzed. The way in which the image is captured also differs among vendors. None involve the inking of the fingerprint as traditional law enforcement procedures often entail.

Fingerscanning can be used for both verification and recognition purposes. At present, the one-to-many identification IAFIS or AFIS applications are confined to law enforcement, government programs and the military. However, there is mounting pressure to expand identification applications. For example, in Toronto, the public was invited to bring their children in for a free "youth print" at a shopping centre one Saturday. A local newspaper ran an item that said: "The fingerprints can be used in the future for identification in a variety of circumstances."[40]

In the areas of financial transactions, network security, and controlling the movement of individuals, fingerscanning is considered to be a highly mature biometric technology with a range of proven installations. Examples of consumer applications include:

- At the beginning of 1999, the Bank of America started a pilot program that uses fingerscans to give customers access to their online banking services. Before using the system, the customer enrols a fingerscan on a chip attached to a multi-application smart card. Authentication is completed by the customer placing a finger on a scanning device attached to their personal computer. The software matches the fingerscan from the scanner against the image stored in the smart card.[41]
- In 1998, it was reported that Canadian banks were looking at thumbprinting cheque-cashing non-account customers.[42] Reportedly, banks in all 50 American states have some version of a fingerscanning system.[43]
- Recently, one American hotel chain announced that it will start collecting fingerprints as part of its check-in procedure.[44]
- A number of vendors have developed fingerscanners resembling a computer mouse. Scanners built into computer keyboards also have been produced. Recognition of a fingerscan takes place in an average of two seconds on a personal computer or one second on a workstation, with accuracy claimed to be 99.9%.[45]

Hand Geometry

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.[46]

In Ontario, hand geometry is used at nuclear power generating stations.[47] Perhaps the best known government application is the United States Immigration and Naturalization Service's Passenger Accelerated Service System (INSPASS). It uses hand geometry readers to verify air travellers' identity, and is currently operating at Toronto's Pearson International Airport.

Hand geometry is predominantly used for one-to-one verification. It is one of the most established biometrics in commercial use today. Applications continue to grow because it is easy to use and convenient. It is also fast, with one vendor reporting a 1.2 second scan.[48] Applications include:

- The 1996 Summer Olympic Games in Atlanta used hand geometry to identify and secure approximately 150,000 athletes, staff, and other participants.[49]
- 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.[50]
- An American elementary school uses the technique to identify individuals picking up children. Anyone authorized 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.[51]
- In Toronto, hand geometry is used by a racquet and fitness club to verify identity of 12,000 club members and staff.[52] Initially, it was introduced at only one location to test acceptability. Now it has been expanded to all locations.[53]

Finger Geometry

This technology operates on similar principles as hand geometry, but utilizes 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."[54] According to one company, its system confirms identity within one second.[55] Finger geometry systems are considered very durable and able to cope well with external conditions.[56] As an example, Disney World uses three-dimensional two-finger geometry to verify the identity of season ticket holders in the United States.[57]

Signature Verification

This behavioural biometric involves the analysis of the way in which a person signs their 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 analyzed as unique behavioural characteristics.[58] 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.[59]

A few years ago, the Chase Manhattan Bank tested DSV to identify corporate clients initiating transactions. Today, a number of American hospitals, pharmacies and insurance firms use this biometric technique to authenticate electronic documents.

Speaker Verification

Voice-related biometrics should not be confused with speech recognition computer software that recognize words as they are spoken. Biometric systems involve the verification of the speaker's identity based on numerous characteristics, such as cadence, pitch, and tone. Speaker verification is 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 user.

One-to-one verification is the preferred application. The technology is easy to use and does not require a great deal of user education. However, background noise greatly affects how well the system operates. Speaker verification works with a microphone or with a regular telephone handset. It is well suited to telephone-based applications where identity has to be verified remotely.[60] In 1997, when one Canadian bank undertook customer surveys on the acceptability of biometrics, the one technique that was not rejected was voice recognition.[61]

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.[62] Voice recognition also is being integrated into security systems for online banking and electronic commerce.[63] One European automobile manufacturer even investigated the possibility of incorporating speaker verification into its ignition systems.[64]

Keystroke Dynamics

Typing biometrics are more commonly referred to as keystroke dynamics. Verification 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.[65] The technique works best for users who can "touch type."[66] The health and fatigue of users, however, can affect typing rhythm.[67]

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.[68] Reportedly, the technology can be used with any keypad, "from computer keyboards to ATM machines to telephones."[69] Previously, differences in keyboards had been one of the problems that had limited the implementation of keystroke dynamics.

Other Developments

Some other techniques are currently being used by law enforcement and the military. While it is not inconceivable that use of these will eventually filter down, it is unlikely that the Canadian consumer will see them in commercial applications in the near future.

Palm Print

This is a physical biometric that analyzes the unique patterns on the palm of a person's hand, similar to fingerprinting. Palm biometrics are predominantly used for one-to-many identification. Like fingerprinting, latent or ink palm images can be scanned into the system.[70]

Vein Patterns

This physical biometric analyzes the pattern of veins in the back of a person's hand. One proprietary system focuses on the unique pattern of blood vessels that form when a fist is made. The underlying vein structure, or "vein tree" can be captured using a camera and infrared light.[71]

Ear Shape

A lesser-known physical biometric is the shape of the outer ear, lobes, and bone structure.[72] 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.[73] One French company is working on the Octophone, a telephone-like biometric device that captures images of the ear.[74]

Body Odour

This is another physical biometric under development which analyzes human body smell. Sensors are capable of capturing body odour from non-intrusive parts of the body such as the back of the hand. Each unique human smell is made up of chemicals which are extracted by the system and converted into a template.[75] Reportedly, the University of Cambridge worked on an "electronic nose" that can identify people by their body odour.[76]

DNA

DNA is an abbreviation of deoxyribonucleic acid. While it is a unique, measurable human characteristic, it is not currently considered a biometric technology.[77]

> Analysis of human DNA, although now possible within ten minutes, is not sufficiently automatic to rank DNA as a biometric technology. When technology advances so that DNA can be matched automatically, in real time, DNA may emerge as a significant contender against the existing biometric industry.[78]

The use of DNA in the areas of forensics and law enforcement has been much in the news with several high profile cases where DNA played a critical role in determining guilt or innocence. Recently, there has been a growing demand to expand the use of DNA. For example:

- Last year, after the Swissair plane crash off the coast of Nova Scotia, the Royal Canadian Mounted Police and prominent forensic experts called for the creation of a global system of DNA samples for airlines crews and possibly frequent fliers.[79]
- The Florida Department of Law Enforcement offered parents a free children's DNA identification program in some of its school districts. Also, Florida is encouraging parents to take DNA samples from their newborns.[80]

Industry Growth

While only a few of the biometric applications mentioned above involve Canadian consumers, this situation will most likely change. Various research firms and industry experts anticipate the growth of the biometric industry to be significant in the near future. To illustrate this point:

- One industry study estimated that world biometric identification markets would grow from $103 million (U.S.) in revenues in 1996 to $170 million (U.S.) in 2003 — a compound annual growth rate of 7.5% over the forecasted period.[81]
- Another study said that biometrics would expand to become a $1 billion industry by the year 2000.[82]
- Biometrics have been identified as one of the ten most critical technologies of the next decade.[83]
- In 1997, Bill Gates of Microsoft Corporation, predicted that biometric technologies would be one of "the most important IT innovations of the next several years."[84]
- Some experts predicted that the rush to install biometric security systems would replace the Year 2000 computer crisis as the most pressing high-tech project after the millennium.[85]

Regardless of the prediction, it is clear that the use of biometrics in the commercial environment is expanding world-wide. It is highly unlikely that Canada will be exempted from this trend.

A number of factors appear to be driving the growth of the biometric industry. One is that, for the most part, the technology itself has matured and generally improved in accuracy and reliability.

Another factor is the recent efforts to create standards for biometric software and programming. Standards will help biometrics gain broader support within the information technology industry as a whole. Recently, the International Computer Security Association certified biometric products for the first time. Standards also will enable differing biometric technologies to function within a single application, with a minimal amount of integration.

While large-scale biometric recognition systems remain relatively expensive, technological improvements have been accompanied by a significant decline in costs. Falling prices have accelerated the absorption of biometrics into information technology.[86] Now biometrics are being integrated into existing operating systems, products and platforms,[87] or offered as "plug-in" or "shrink-wrapped" products that easily can be added to computer and security systems.

This trend has increased consumer awareness and adoption. With dozens of low-cost biometric systems appearing on the market last year, some believe biometric technology is moving into the "electronic mainstream of personal computers."[88]

The most influential development has been the expansion of electronic commerce and the Internet. This has greatly increased corporate concern about security in general, and network access in particular.[89] The recent explosion in the electronic commerce market has been accompanied by a countervailing growth in fraud, hacking, and other security concerns.

As more and more transactions become remote, the need to authenticate business parties becomes more difficult. The nature of electronic commerce impairs each party's ability to identify the other with certainty.[90] Online transactions make it easier to impersonate, mislead, or "spoof" an identity.

In addition, as more information is sent over networks, the need to secure that data against interception and alteration increases. Data integrity concerns become paramount. The Internet is perceived as extremely vulnerable by the businesses that use it. An Ernst & Young 1997 survey found that nearly one in four businesses were staying away from the Internet because of worries about security.[91]

Today, major high-tech companies consider biometric technology as a viable and cost-effective way of offering the security and privacy protection demanded by their electronic commerce clients. Last year, Novell, Compaq, IBM, Hewlett-Packard, and Microsoft all invested resources in biometric applications. In 1998, manufacturers of guns, locks, ATMs, automotive security, and medication dispensing devices also introduced products or prototypes that may be accessed by biometrics.

Benefits

Biometric technology offers a number of benefits to both businesses and consumers. It is these benefits, in addition to the factors noted above, that are driving their increased usage and acceptance.

Positive Identification

Companies are looking to biometrics because they see the positive identification provided by the technology as a way to: control fraud and abuse, build non-repudiation into electronic commerce transactions, and to enhance customer service.[92] It can be reasonably argued that each one of these potential corporate benefits also benefit the customer.

In today's business environment, many organizations can no longer rely on their employees to recognize individual clients. Companies are looking for means whereby individuals can be recognized reliably, at a distance, over a period of time, without reliance on human memory, and, in some cases, despite the preference by the person not to be recognized.[93]

Financial institutions have long been evaluating the merits of biometrics. This interest has increased significantly with the rise in electronic banking. It is estimated that over 85% of all banking transactions are now done electronically.[94] A January 1999 survey revealed that over the last year 76% of Canadians used ATMs, while 43% were concerned about the security of electronic commerce transactions.[95]

ATMs and transactions at the point-of-sale are considered to be particularly vulnerable to fraud and breaches in security. Emerging markets such as telephone and Internet banking also need to be secured for bank customers and bankers alike.[96]

Biometrics are seen as ideally suited for electronic commerce and other online applications because they can automatically "prove" the identity of a person while ensuring that no-one else can impersonate them.[97] The benefit of positive identification is strengthened by the fact that biometrics can connect an actual person to a transaction. By linking a verified individual to a particular transaction (much like a digital signature), repudiation by a party after the fact, on the grounds that the identification was forged, becomes very difficult.[98] Biometric authentication systems "can be built using an online signing service to accept the biometric measurements, and if the identification is positive, to use the secret key on behalf of the user to generate the cryptographic binding of the document to the identity of the user."[99]

Combatting Credit Card Fraud

A significant sub-set of the identification issue is credit card fraud. According to the Canadian Bankers Association, credit card fraud was $147 million in 1998, compared to $127 million in 1997.[100]

Stolen credit card numbers are routinely posted and swapped on Internet bulletin boards and real-time chat lines. On the Internet, credit card numbers come from traditional offline sources (e.g., stolen wallets and discarded receipts), as well as from poorly-secured web servers that store credit card information.

Now there are computer programs that fraudulently generate valid credit card numbers. All credit card numbers end with a "check-sum" digit that is generated from the other digits using an algorithm. That formula is used by these programs to create unauthorized numbers that can fool a simple authorization check.[101]

A recent American survey found that nearly one-third of consumers who have bought products on the Internet have experienced fraud or misuse of credit card information.[102] According to a February 1998 survey, 87% of Canadians would not provide their credit card number over the Internet to purchase a product or obtain a service.[103]

Requiring positive identification of the cardholder prior to authorizing a transaction (either in person or online) has obvious appeal to sponsoring financial institutions, as well as to individual businesses. Canadian consumers also are concerned about credit card fraud, and could be in a position to benefit from the use of a biometric. MasterCard International estimated the use of biometrics could reduce credit card fraud by 90%.[104]

Preventing Identity Theft

The need for accurate identification is as important an issue for consumers as it is for businesses. Fuelling consumer interest in biometrics is the rise of identity theft — a crime resulting from the misappropriation and abuse of personal information.

Identity theft, also known as identity fraud, includes a range of crimes broadly defined as "the misuse of personal identifying information to commit various types of financial fraud."[105] In the United States, identity theft has been described as "the fastest growing crime in the nation," and "the leading form of consumer fraud."[106]

Identity theft involves unauthorized parties acquiring key pieces of a person's identifying information in order to impersonate them and spend as much money, in as short a time as possible, before moving on to someone else.[107]

The theft of identity can leave someone with a poor credit rating and a ruined reputation that may take months or even years to correct. Meanwhile, due to their seemingly bad credit history, they may be denied loans, cheque-writing privileges, the right to rent accommodation, obtain a mortgage, and perhaps even a job. They may even risk false arrest in place of their imposter.

While there are many ways to combat identity theft,[108] some consumers see biometrics as an effective and convenient way to diminish the problem. Biometrics can fight identity theft by eliminating PINs and passwords, by verifying the identity of parties in a remote transaction, by authorizing credit card or cheque transactions, and by securing personal assets like computers, as well as personal information. In this capacity, a biometric can be seen as an identity *protector*.

One new service, called e-DENTIFICATION, is designed to help allay consumer concerns about participating in electronic commerce for fear of identity theft or misuse of their personal information. It is set up so that each individual identity record is biometrically "passworded" and encrypted, with the key remaining in the consumer's control. The identity record is "legally owned and controlled by the individual consumer and cannot be accessed without the biometric consent of the consumer."[109]

With the rise of identity theft, the imperative for identity authentication has changed from just being a corporate concern to one shared equally by consumers. Now, more than ever before, it is critical for consumers to be able to prove their identity. In order for individuals to protect their own identify from theft or misuse, they need a secure form of portable identification that they control. Biometrics offer this potential.

Restoring Identity

Biometrics offer another potential benefit to consumers in that they can verify their identity should their identifying papers be lost or stolen. The technology addresses the "chicken or egg" question of how does a person get identification if they have no identification. An example illustrating the utility of biometrics may be found in Oklahoma where authorities issued new driver's licenses with a thumbprint, to replace documents lost in tornadoes. The biometric was seen as a deterrent to criminals, and a way to protect the public by ensuring that the new licenses were given to their rightful owners.[110] Should these licenses be lost in the future, the biometric will re-establish identity so the appropriate person can be issued the necessary documentation quickly and easily. This benefit is equally applicable to membership or credit cards.

Enhanced Security

The changing nature of business has created significant new security concerns. With customers increasingly interacting with companies through some form of information technology (e.g., telephone, kiosk, or computer), traditional security methods are being challenged. Opening up access to computer systems and networks may enhance customer service, but it also increases the potential for security breaches. A 1999 survey on computer crime in the United States indicated that almost one-third of respondents reported that outsiders had penetrated their computer systems in the past year, most frequently through an Internet connection. The most serious losses occurred through the theft of proprietary information and financial fraud.[111]

As noted earlier, traditional authentication methods involve something the user *knows*, such as a password or PIN, or something the user *has*, such as a card, key, or token. Now companies are questioning the reliability of these security measures to protect their interests, as well as those of their customers.

Cards or keys can be forgotten, given away, lost, stolen, duplicated, or forged. Passwords can be shared, guessed, observed, stolen, or forgotten. One example of the limits of passwords is that a group of hackers from Europe broke into the e-mail system at Stanford University in California, stole thousands of student and staff passwords, and went undetected for three weeks.[112]

A 1999 survey found that even experienced computer users tend to choose the same passwords. The most popular were dates of birth (15%), and names of partners, children, or pets (49%), while 20% of the men surveyed chose their favourite football team. Eighty percent (80%) of respondents justified choosing simple passwords because they were afraid of forgetting more complex words and number combinations.[113]

New computer viruses can capture keystrokes so that as a person types their password or PIN, including their encryption keys, the software collects and transmits that information to unauthorized parties, without the authorized user's knowledge. Keystroke recorders or loggers are designed to record and play back all keyboard and mouse action. These programs are widely available yet difficult to detect, with some having the ability to penetrate conventional firewall protections.

Some industry experts predict that the use of passwords for e-mail, corporate networks, and the Internet will come to an end in the next few years. Passwords are seen as being far too vulnerable, while biometrics are seen, by some, as offering superior security.[114]

Biometric companies are promoting their products as security systems that cannot be stolen, forgotten, shared, or intercepted. Additionally, biometric characteristics can only be linked to a single identifiable individual. The technology offers two significant advantages over other authentication methods:

- the person to be identified is required to be physically present at the point-of-identification;
- identification based on biometric techniques eliminates the need to remember a password, PIN, or carry a token.[115]

Some industry supporters consider biometrics to offer "the most effective information security tool."[116] The reason is that biometric systems verify the person, not the card or the code.[117] This advantage has led vendors to call the technology "proof positive" security.[118] Biometrics are considered to be particularly effective when several techniques are layered (e.g., voice verification and fingerscan),[119] or combined with traditional security measures. The security claims of the biometric vendors are discussed further under the General Issues section of the paper.

The potential for enhanced security offered by biometrics to businesses regarding their computers and networks has a flipside for consumers. A customer is just as concerned about the validity and security of an online transaction.

Data Authentication

To prevent the unauthorized altering of information (deliberate or unintentional) during online transactions, some form of data authentication becomes necessary. This ensures that the information sent and received is complete and not tampered with or intercepted in transit.

The use of encryption to secure both business and personal communications is on the rise. Encryption is a mathematical process that changes data from plaintext (i.e., that which can be read) to an unintelligible form. In order to reconstructed the original data or decrypt it, the key to the algorithm used must be known.

Certain newer biometric systems can be used to encrypt data — the process is called biometric encryption.[120] Information extracted from a biometric can be used as the key to scramble and unscramble data. As an example, the unique pattern in a person's fingerprint could be used to code his or her PIN for accessing a bank machine. The coded PIN has no connection whatsoever to the finger pattern. What is stored in the database is only the coded PIN. The finger pattern acts as the coding key. The actual fingerprint pattern is not stored anywhere during this process. Biometric encryption ensures that the information encrypted with the biometric key cannot be decrypted without the live biometric. Another potential benefit to this system is that the operation of successfully decoding the PIN authenticates that person's eligibility for the service, without having to reveal any personal identifiers.[121] Most importantly, biometric encryption cannot serve as a unique identifier, eliminating many fears commonly associated with the use of a biometric, as discussed later in the paper.

Physical Access Control

Initially, biometric access controls were limited to high security areas such as nuclear power plants and military facilities. Now, these access control systems are used in theme parks, hotels, and health clubs. Some industry commentators believe there is no limit to the kinds of organizations that could use biometrics to secure the physical movement of people, particularly as prices continue to fall and public acceptance grows.

Automated access control systems using biometrics offer certain advantages over keys, cards, or security guards in terms of convenience, security, and operating costs. Forgotten passwords and lost keys or cards are a nuisance for users, and a major expense for the company.[122] With the existing demographics of our aging population, memory loss only can be expected to escalate.

From a business perspective, the benefits of a biometric access control system are that access can be limited by person, by location, and by time, and the system keeps an accurate record of exactly who is given access and when.[123] Biometric systems are viewed as being reliable and constant, since machines never get distracted, tired, or are affected by the "psychological defects" that may affect security guards.[124]

From a consumer's perspective, biometric systems designed for large-scale access control are fast and easy to use. In addition, consumers can benefit from customized service and the convenience of 24/7 access. If one thinks of all the PINs, passwords, and cards one uses throughout the day to access an office, computer, bank account, or health club, it is easy to understand why biometrics are appealing to many people. Nothing to remember, nothing to carry. A person simply presents their biometric to be authenticated and is given access.

Another potential consumer benefit to the technology is that it can give people control over their own assets and information. In certain circumstances, such as with the above-noted biometric encryption, individuals can use a biometric as their own access control measure. This means they can put their own confidential information somewhere, both off- and online, and then secure it with their biometric. No one but they can gain entry.

General Issues

From the preceding discussion, it is clear that biometrics can offer a number of significant benefits to both businesses and consumers. However, in order to make an accurate assessment of biometrics, those benefits should be considered in conjunction with a number of issues or problems associated with the technology. Chief among these are the privacy concerns, which are outlined in the next section.

Biometrics vary with regard to ease of enrolment and use, accuracy, costs, speed, public perception or acceptability, and long term stability (i.e., how time affects the physical or behavioural characteristic). Comparisons of these and other factors for the different biometric techniques have been performed by a number of sources.[125] Consumers should realize that not all biometrics are appropriate for all applications.

The purpose of the discussion here is to make consumers, and others, aware of some of the general performance and security issues related to the technology itself.

Performance

The first thing that consumers should understand is that biometric systems do not guarantee 100% accuracy, 100% of the time. Commercially available biometric systems allow for some degree of variability in the measured characteristic or trait and update the referenced sample after each use.[126]

> The biometric system must allow for these subtle changes, so a threshold is set. This can take the form of an accuracy score. Here, comparison between the template and new sample must exceed the system's threshold before a match is recorded. In other words, if the new biometric sample is considered by the system to be sufficiently similar to the previously stored template, the system will determine that the two do in fact match. If not, the system will not record a match and will not confirm identity.[127]

While the threshold is set to accommodate some variation, the challenge is to set it so that the system only matches authorized individuals. Two potential problems can arise:

- **False Rejection:** This is when an authorized individual is rejected by the system.
- **False Acceptance:** This is when the system accepts an unauthorized individual.

Set the threshold too high and legitimate users will fail to be identified. Set the threshold too low and unauthorized users will be accepted. There is usually a trade-off between these settings, where reducing the false rejection rate will simultaneously raise the false acceptance rate.[128]

Where this threshold is set depends upon the purpose of the biometric system and the degree of security required. For example, military personnel or workers at a nuclear facility may have to accept the frustration of repeated false rejections in order to secure a sensitive installation. The same rate of rejection would be unacceptable for admission to a theme park by paying customers or at an ATM. In consumer applications, false rejections could create serious customer service problems.[129]

Variations in Characteristics and Traits

No single biometric can be used for the entire population of users in all circumstances. A percentage of users will have missing or damaged biometric characteristics. This makes automatic identification or verification of all users with a single biometric system impossible.[130] For this reason, alternative and appropriate methods of verifying identity for those unable to utilize the biometric should be an important component on any system.

In addition, both physiological and behavioural characteristics can vary over time. For example, hands can swell from work, heat, or allergies; fingerprints can be marred by scratches, exposure to chemicals, or embedded dirt; voices can vary from colds; and signatures may change as a person gets older. General factors such as stress, health, environmental conditions, and time constraints also can impact the interaction between the person and the machine and can lead to inconsistencies.[131]

Behavioural characteristics are more susceptible to variations in execution than physiological traits. For example, a person can vary their voice (intentionally or otherwise) much more readily than they can change their fingerprint. Comparative studies on various biometric techniques show a lower level of accuracy in behavioural biometrics, than with physical characteristics.[132]

User Attitude

How users feel about the biometric system can also impact performance.[133] Some individuals are "technophobic" or have other personal reasons for being concerned about using a biometric system. The intention and overall co-operation of the user, as well as the way a person interacts with a system, may affect its accuracy. The first time a person uses a system will be different from the tenth time. Each of the ten biometric readings will be unique. Generally, if a co-operative user becomes more familiar with a biometric system, the quality of data capture will improve.[134]

Some techniques are generally more acceptable to people than others. As an example, one study found iris and retinal scans to be the most unacceptable; fingerscans, hand geometry, and hand vein recognition more acceptable; and face, signature, and voice recognition, as well as thermograms, the most acceptable.[135] People's acceptance of biometrics is based on perceived intrusiveness, speed of enrolment and use, and similarity to other familiar

processes. For example, people can be concerned about a retinal scan because it involves shining a beam of light into their eye. In addition, it requires precise alignment and a pause while the scan is done. Due to the level of unease this can cause with some users, one study showed the data collection error rate for retinal scans to be considerably higher than for fingerprints.[136] Some other biometric techniques can be done in a more "natural and casual manner,"[137] such as dynamic signature verification.

Uniqueness

The degree of "uniqueness" varies among the different types of biometric characteristics. While vendors may claim their systems use unique characteristics, in actuality, uniqueness is measured by statistical probability. Some industry analysts maintain that, with the exception of fingerprints, biometric characteristics have not been demonstrated to be unique.[138] Others accept retinal and iris scans, in addition to fingerprints, as truly unique because there are no documented cases of duplicates.[139] What is considered to be unique will continue to evolve as new techniques are introduced and tested.

The degree to which a biometric characteristic must be unique in order to accurately identify users depends on the type and size of the application. In small applications, the uniqueness of the biometric feature is less important. It may be sufficient for the feature to just be "very unlikely" to be duplicated. In large applications, systems based on non-unique features may be more likely to have false positives due to similarities.[140]

One of the factors influencing the uniqueness and, therefore, the accuracy of the different biometric techniques is the amount of data collected and compared. One estimation of the data quantity per record is nine bytes for hand geometry, 35 bytes for retinal scans, 265 for iris scan, and between around 500 to 1000 for fingerscans. This is one of the main reasons why fingerprints are so widely adopted by the law enforcement community. One estimation has the fingerprint identification process in AFIS applications as having a 98%+ identification rate and the false positive identification rate is less than 1%.[141]

A biometric with a small data size per record may not be the most accurate in a large scale identification application that would involve a search of all available samples, perhaps numbering in the millions. Given the small per record size, there would be a high probability that a particular record would have an identical, or nearly identical, match in the database. Discriminating one record from among many identical or near identical records would be difficult to achieve.[142] What this means is sometimes a particular technique is not appropriate to an application. Some are better suited to one-to-one matches, while others can perform accurately and reliably in a one-to-many match.

Testing

Biometric vendors offer performance figures for their systems. Consumers should understand that these quoted performance figures only apply to the specific application and circumstance under which the system was tested. There is often a wide variation in the false rejection rates (FRR) and false acceptance rates (FAR) achieved from in-laboratory testing compared to an "in-the-field" application.[143]

There also may be a significant variation in the performance figures quoted by vendors and those identified through independent testing.[144] As an example, the performance of one biometric system was claimed, by its manufacturer, to have a FRR of 0.3% and an FAR of 0.1%. An independent test found the system had a FRR of 25% with an unknown FAR.[145] With the development and adoption of standards, and the establishment of certification programs and independent testing facilities, consumers can anticipate that performance figures will become more reliable and consistent in the future.[146]

Security

There is general acceptance that biometrics offer enhanced security over knowledge-based and token-based identification methods, as outlined in the previous section. However, it is important to understand that biometrics are not invincible. The level of security varies according to the type of biometric characteristic used and how they are applied. There are strong and weak biometrics from a security perspective.

Generally biometrics are considered secure because they are based on the premise that only someone with an identical face, iris, voice, fingerprints, or whatever, can impersonate another person. Since this is considered to be "impossible," the systems are considered to be secure.[147] However, the reality is that certain biometric techniques are more easily spoofed or circumvented (i.e., fooled by fraudulent means) than others. For example, there are reported cases of twins fooling face recognition systems.[148]

Two different types of impersonations are a consideration:

- **Active Imposter Acceptance** — when an imposter submits a modified, simulated or reproduced biometric sample, intentionally attempting to relate it to another person who is an enrollee, and he/she is incorrectly identified or verified by the biometric system as being that enrollee.
- **Passive Impostor Acceptance** — when an impostor submits his/her own biometric sample and claiming the identity of another person (either intentionally or inadvertently), and he/she is incorrectly identified or verified by the biometric system.[149]

One important distinction between biometric characteristics is whether they are open or closed view. "Open view" biometric traits are those that can be easily recorded or photographed, or are left on every item a person touches, and, as a result can be covertly captured

(e.g., fingerprint). Some can be worked on by criminals until satisfactory facsimiles are produced to fool or spoof a biometric system. "Closed view" traits are hidden or internal biometric parameters as well as certain behavioural characteristics, that can be more difficult to illicitly capture or reproduce (e.g., keystroke dynamics or vein patterns).[150] Accordingly, open biometrics are considered easier to steal and impersonate than closed biometrics.

One study rated the level of difficulty of biometric circumvention as follows:

- **Low:** signature, voice, and face recognition
- **Medium:** hand geometry
- **High:** fingerprint, thermogram, iris and retinal scan.[151]

A review of selected biometric products by *PC Magazine Online* also illustrates the variation between techniques. The magazine subjected a number of products to a series of tests to determine how securely and efficiently they could authenticate users. It was successful in breaking into a voice authentication system by mimicking the voice of the enrolled user. For face recognition, it was able to "fool" the systems tested with a mask created with a colour printout of a digital photograph. A three-dimensional aspect to the mask was added by cutting a nose hole and placing an impersonator's nose similar to that of the real enrollee through the hole. For the fingerprint recognition systems tested, the magazine used various methods (e.g., it rolled a print onto a fingerprint card and then pressed the image to the reader, it used an ink fingerprint on a latex glove, and finally it dusted for latent prints and then lifted them on tape and presented them to the reader). All methods used were unsuccessful. *PC Magazine* noted: "Our lack of success is a reflection of the relative maturity of fingerprint recognition technology, which has been in use in a number of environments for decades."[152]

All of the performance factors, noted above, are relevant in determining the degree to which biometric systems can be fooled. Another important factor is where the threshold between FRR/FAR levels is set. Different applications using the same biometric characteristic or trait can offer different levels of security.

Despite these examples of spoofing, it must be acknowledged that it is very difficult, even impossible, for someone to forge an actual biometric characteristic. However, it is much easier for someone to copy a digital image of a person's biometric. One security expert has said "it's easy to steal a biometric after the measurement is taken."[153] Consumers should be aware that, as biometrics are used in more and more online applications, a significant security problem could arise.

To recognize or verify the identity of an individual, a biometric system always requests the same information — information that is designed to remain relatively static over time. Due to this design feature, some security experts maintain that all biometrics devices are susceptible to a "replay attack" if an intruder is able to make a copy of the description of the legitimate user's characteristic. Once a biometric has been digitized, it can be compromised and intercepted without proper security controls. This type of attack requires some access to the software or network connection, making remote applications more vulnerable than local.[154]

Every biometric box has a wire coming out of it that carries either the description of the eyes, fingerprint, or whatever part of the body is being measured [or a yes/no digital message that indicates whether the correct biometric was presented]. Hacking the system is simply a matter of cutting the line and splicing a digital tape recorder in place. If you want to be John Smith, just replay his tape. In many cases, you don't really need to cut any wires. It can all be done virtually by hacking around in the lower realms of the object system.[155]

An "identity thief" does not need the actual biometric characteristic to impersonate someone. They only need to capture the digital image of that person's biometric.[156] Unless the owner of the biometric has to be observed when their live scan is read, or there is some additional authentication measure used, the computer will not be able to distinguish the difference.

This raises a number of significant security concerns related to this vulnerability. As more biometrics are used in the commercial environment, particularly in conjunction with the Internet, one author suggests "… the question you have to ask is do you want to have your fingerprint, or whatever, floating around on the Internet. It is not like a credit card on the Net, as you can't just cancel or replace it if it is lost or stolen."[157] A person can think of new passwords or PINs, but once their biometric is compromised, they cannot get a new one.

> Imagine that Alice is using her thumbprint as a biometric, and someone steals it. Now what? This isn't a digital certificate, where some trusted third party can issue her another one. This is her thumb. She only has two. Once someone steals your biometric, it remains stolen for life; there's no getting back to a secure situation…
>
> [Another] more minor problem, is that biometrics have to be common across different functions. Just as you should never use the same password on two different systems, the same encryption key should not be used for two different applications. If my fingerprint is used to start my car, unlock my medical records, and read my e-mail, then it's not hard to imagine some very bad situations arising.[158]

It has been suggested that biometrics are only secure "if you have an armed guard watching the biometric reader. Otherwise it can be fooled."[159] In order to eliminate the potential for replay attacks, biometric systems should be properly configured with secure biometric readers where authorized people directly present their biometric, or where biometrics are integrated into other security devices, such as smart cards.[160]

Another possible solution may be the use of biometric encryption. As noted earlier, what makes most biometric systems vulnerable to a replay attack is that they always ask the same question: "What is your left index fingerprint?" The response to that unchanging question is also always the same. To thwart a replay attack, a biometric system would need a "challenge and response" system that would ask different questions each time and be able to measure the correct response.[161]

The use of biometric encryption may be able to improve security of biometric systems by introducing a type of challenge and response system, by generating one-time passwords for each access, as follows:

> The response function can be coded by the finger pattern. The coded response function is then stored on a memory card. To authenticate, the host system transmits the challenge which serves as the argument to prompt and calculates the value of the response function. The coded response function is decoded by the finger pattern, allowing the response to be calculated and transmitted to the host for evaluation.[162]

The purpose of raising these performance and security issues here is to alert consumers to the fact that, in order to make a critical evaluation of the technology, they should not get caught up in the rhetoric of the industry. "Biometrics is not a panacea."[163] Many variables affect the performance and security of the different biometric techniques. However, given the potential benefits offered by biometrics, consumers can anticipate that the industry will make continued efforts to address these security issues, particularly as the online world expands. Until satisfactory solutions are implemented, caution is advisable.

Privacy Concerns

Before discussing the specific privacy concerns raised by biometrics, it is important to understand that privacy is a highly subjective notion. It means different things to different people. While the right to privacy is not explicitly guaranteed under the Canadian *Charter of Rights and Freedoms*, there is a common understanding that privacy should be valued and protected. Indeed, the Supreme Court of Canada has recognized the value of privacy:

> … Grounded in man's physical and moral autonomy, privacy is essential for the well-being of the individual.[164]

The House of Commons Standing Committee on Human Rights and the Status of Persons with Disabilities studied privacy and concluded that:

> Canadians view privacy as far more than the right to be left alone, or to control who knows what about us. It is an essential part of the consensus that enables us not only to define what we do in our own space, but also to determine how we interact with others — either with trust, openness and a sense of freedom, or with distrust, fear and a sense of insecurity.[165]

The Canadian Task Force on Privacy and Computers identified and defined several component parts of privacy. Two of these concepts are relevant to this discussion, and will be used to describe the privacy concerns associated with biometric technology.

- **Privacy of the Person:** This is the idea that a person should be protected against unwarranted intrusions. It encompasses not only protection against physical harassment or search or seizure of the person, but also extends to protection of the dignity of the person.
- **Informational Privacy:** This is the idea that information about an individual belongs, in a fundamental way, to that person, and is to be communicated or not, as the individual determines.[166] This concept is also known as informational self-determination.

Privacy of the Person

Any form of identification may attract opposition in different circumstances. However, as one author noted, "The greatest degree of public distrust … is generally associated with biometric identifiers. Their use is in some cases invasive, and in all cases seems that way."[167]

To some people the need to identify themselves is intrinsically distasteful and demeaning. It is symbolic of the power that an organization they are dealing with has over them. Having to present a biometric is considered by some, not just a form of moral submission to authority, but also physical submission.[168] To them, biometric identification represents the ultimate invasion of personal privacy.

The very nature of biometrics raises privacy of person issues for some people. Having to give something of themselves to be identified is viewed as an affront to their dignity and a violation of their person. Certain biometric techniques require touching a communal reader, which may be unacceptable to some, due to cultureal norms or religious beliefs. Others are apprehensive about interacting with a machine because they are not familiar with the technology, or are afraid that biometrics may cause them discomfort or harm.

As noted earlier, the biometric techniques that have gained the most user acceptance are fast, easy to use, and perceived as the least intrusive, such as fingerscan, hand geometry, and facial recognition systems.[169] There is no evidence that any biometric system has adversely affected or injured a user.[170] In addition, no commercially used systems present health risks, or leave marks, or take physical samples from users.[171]

Use of biometric identification is interpreted by some as a questioning of their reputation and trustworthiness. They perceive a requirement to give a biometric as a reversal of the presumption of innocence — as shifting the burden of proof. Without pre-existing evidence of wrongdoing, organizations are requiring them to sacrifice their personal privacy.

These privacy-of-the-person concerns are exacerbated by the fact that fingerprints are strongly associated with law enforcement. As a result, a requirement for the provision of fingerprints can be seen, not only as an invasion of privacy, but also as an indignity and an embarrassment.[172] Some people feel they are being treated like criminals.

However, it should be noted that this concern does not appear to be shared by the majority. For example, one American survey found that 87% of respondents thought fingerprinting was a legitimate identification requirement, 91% believed that the use of finger imaging was justified 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.[173]

There has been very limited public opinion research into how the Canadian public regard biometrics. In Ontario, a 1997 survey about a proposed provincial identity card indicated that 60% would consent to being fingerprinted for a social program in order to fight fraud.[174] Although this context is quite different from use by businesses in the private sector, the results do show a recognition by the public that the use of biometrics in certain circumstances is considered to be justified.

Informational Privacy

A 1998 Canadian newspaper poll asked if biometric technology was a threat to privacy — 51% of respondents said yes.[175] The majority of privacy concerns about biometrics relate to informational privacy and the ability of a person to determine when, how, and to what extent their biometric information is communicated to others.

However, associated with biometrics is a high level of general anxiety about privacy because the technology can reveal information that is so intimate and intrinsic to oneself. Some people have the view that biometrics, "much more so than other identification schemes, may imperil the sense of individuality."[176] It is necessary to first understand this concern, in order to put the specific informational privacy issues into context.

Big Brother

An overarching concern for some people is that biometrics will become a technology of surveillance and social control. Perhaps as the ultimate personal identifier, it can be seen to facilitate all the ominous and dehumanizing aspects of an information society — a society in which unparalleled amounts and specificity of personal information is collected and used on a systematic basis.

Findings of repeated surveys show that Canadians feel vulnerable in the face of invasive and unrestricted information technology and practices, and believe they are losing their personal privacy.[177]

Today, more than ever before, it is clear that information is a valuable commodity and a source of power. More and more, people are defined by their "data image," or the information stored about them in computer databases. This raises the fear that information technology puts the "power to know" into the hands of those who control the technology.[178]

The feeling of helplessness against increasingly powerful computers arises in the context of biometrics because it is a machine that authenticates a person's identity. Misallocation or misappropriation of biometric identifiers is possible, as noted earlier. The digital image of one person's biometric characteristic can be intercepted and used by another. This raises the concern that biometrics may actually entrench false identity. How does one separate oneself from activities authorized by one's own biometric? If a person's biometric, and thus their identity, is stolen, the stored biometric template can take on an almost irrefutable quality.

A major privacy concern is that while biometrics initially will be deployed for very limited, clearly specified, and narrow purposes, inevitably, over time, the use of biometric identifiers will spread. This phenomenon is commonly referred to as "function creep." People are concerned that they may find themselves required to provide a biometric identifier in unexpected, and possibly unwelcome, circumstances.

The central concern is that a biometric can act as a very powerful unique identifier — that it will be used to link all information about a person. "Consider the ease of finding anything you wanted to know about an individual if all of that person's data were tagged with a biometric ID."[179] 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."[180]

Most people are able to go through their days enjoying what are, in essence, different identities. Their work identity need not impact their personal identity. They even have the option of giving a false name on the Internet or other situations.

A biometric is a unary identity: All of us have only one left thumbprint. How will you separate your work identity from your private identity … there is significant risk that your private activities (buying habits, entertainment preferences, political activities) will be inextricably connected to your work activities.[181]

If biometric identifiers are widely used and shared, people's freedom to separate or even choose their identity could be restricted. All information about them could be linked to their biometric. They will always be identified because that is who their biometric data says they are. As biometric authentication devices proliferate, their ability to remain anonymous also will be diminished.

The most extreme concern in this context is that all biometrics will be turned over to the government or law enforcement agencies (aka Big Brother) to amass personal dossiers on all members of society.

> One of the most frightening concerns in the widespread deployment of biometric ID systems is their use to track individuals. Even when not intended for such use, the emergent reliance on biometric ID authentication for a wide array of daily transactions means that law enforcement and others can more effectively follow a person's movement — in real time in some cases. As the cost of biometric readers decreases, these devices will turn up virtually everywhere, leading to an ability to track a person's movement from hour to hour.[182]

Countering this concern are industry experts who think diversity within applications and types of biometric identifiers, as well as the proprietary nature of the systems, make this scenario technically infeasible. One author noted that biometrics can be used to work against Big Brother:

> A fragmented user population made up of companies, government departments and other organizations is unlikely to become an omnipresent autocrat. Indeed, biometrics can be used to brush aside any fears … about the general intrusion of technology into our lives. A combination of encryption and biometrics could actually act as the perfect privacy tool. Biometrics are the ideal key for securing data held in various public and private databases, ensuring that it cannot be merged, thus fighting the concept of Big Brother.[183]

Loss of Control

Generally, people feel the loss of control over their personal information has a significant impact on their ability to be autonomous.

> … not only does the loss of control of information about one's self have some possible serious negative consequences, such as no protection from misuses of the information, it also means a loss of autonomy… Loss of autonomy means loss of one's capacity to control one's life… A right to control information about one's self is fundamental to being a self-determining and responsible being.[184]

Most people acknowledge that companies need to collect, use, and disclose information about their customers in order to conduct business. Consumers generally understand that anything beyond a straight anonymous cash transaction necessitates the disclosure of some of their personal information. This is seen as necessary and reasonable, falling within the expectations of most consumers. Informational privacy issues arise when companies use biometric data for purposes that go beyond customer expectations.

The specific informational privacy concerns associated with biometrics may be summarized as follows:

- **Unauthorized Collection:** Some techniques, such as thermograms, can collect biometric data without the data subject's knowledge. Should such a collection take place, it would be an extreme violation of a person's informational privacy. However, it must be noted that such a practice is far from the norm for consumer applications. Covert collection is generally confined to law enforcement purposes. For a company to achieve the benefits discussed earlier, voluntary participation in biometric verification systems would seem advisable.

- **Unnecessary Collection:** A central tenet of informational privacy is that the collection of personal information must be limited to those data that are absolutely necessary and relevant to the legitimate business function. Positive identification is an important component of information management and security systems. However, a biometric identifier is not always necessary for such systems to be effective.

  Biometrics are considered to be highly personal, and there can be strong emotions associated with their use. Accordingly, when the benefits from their use are not commensurate with the level of risk associated with not using a biometric, people may feel their privacy is being compromised unnecessarily. A recent American survey showed that consumers were reluctant to share certain types of personal information, such as biometrics, unless they saw a "clear benefit."[185]

  Technological improvements in information-handling capability have generally been followed by a tendency to engage in more manipulation and analysis of the recorded data. This, in turn, motivates the collection of data pertaining to a larger number of variables, resulting in even more personal information being collected.[186] The increased capacity of computers to collect, retain, and manipulate information — at limited costs — heightens concerns about unnecessary collection. Companies may collect a biometric identifier simply because it is useful and cost-effective to do so.

- **Unauthorized Use:** When consumers consent to the use of a biometric identifier to unlock a door at a health club, or to access an ATM, they do so on the understanding that their biometric will be used for that specific purpose and no other. Perhaps the greatest fear associated with biometrics is that companies will use them for unrelated purposes (known as secondary use), without someone's consent or knowledge.

  A biometric can be used as a means of bringing together disparate and dispersed personal data on individuals. If used as a universal personal identifier, a biometric not only enables individuals to be pinpointed, but creates the potential for data to be used for purposes not intended at the time of collection, and for the collation of information into a comprehensive profile, unbeknownst to the individual to whom the data relates.

  This fosters the following concerns: that information will be used out of context to the detriment of the data subject; that unjust decisions about them will be made simply on the basis of that profile; that automatic decision-making will be based on facts of doubtful completeness, accuracy, relevance, or utility; and that all of this will be done without the data subject's permission.

  This is of particular concern in the private sector where there are no legislative constraints on the use or misuse of biometrics. When the use of biometrics is left to market forces, the fear is that companies may use biometric data for unauthorized purposes in the pursuit of economic gain.[187]

  It is here that the distinction between identification and identity becomes important. For most people, the simple process of capturing information related to their identification, in and of itself, is not considered to be an invasion of privacy. If, however, the information obtained is used improperly, it ultimately could lead to the loss of one's identity.[188]

  The threat to privacy arises not from the positive identification that biometrics provide best, but the ability to access biometric data in an identifiable form and link it to other information, resulting in unauthorized secondary uses. This erodes a person's control over his or her own information — such control being a fundamental tenet of informational privacy.[189]

  A particularly significant concern regarding biometrics is that the technology will be used to do more than simply verify identity — it may be used by companies for unethical and discriminatory purposes.[190] In particular, a major concern is that biometric information will be used to diagnose medical conditions the individual may be unaware of, with the resulting knowledge being used against them.

  Some industry commentators say: "A biometric system is not built to recognize physical or mental illness … The purpose of biometric technology is automatic identification and verification, not storing medical data for some sinister agenda."[191]

  However, it is certainly technically possible to identify various health and medical conditions from some biometric data. Recent scientific research suggests that finger-

prints and finger imaging might disclose medical information.[192] Certain chromosomal disorders (e.g., Down's and Turner's syndromes), as well as certain non-chromosomal disorders (e.g., leukemia and breast cancer), have been indicated by unusual fingerprint patterns. By examining a person's retina or iris, it can be determined if that individual is suffering from diabetes, arteriosclerosis, or hypertension, as well as diseases of the eye.[193]

This ability raises the prospect of significant privacy violations. A fictitious illustration of this concern would be if an insurance company that used biometric information obtained from its policy-holders for the purpose of enabling them to transact business remotely via the Internet, also used it to make decisions about the policy-holders' eligibility for coverage. Not only would the informational privacy issue of unauthorized secondary use be raised, but the absence of due process also would be an issue. Consumers cannot challenge or refute a decision if they do not know how that decision is being made. If they are unaware of the fact that their biometric has been used to identify medical conditions relevant to a determination of their entitlement to benefits, then they are not in a position to take any action.

- **Unauthorized Disclosure:** Closely related to the issue of unauthorized use is unauthorized disclosure. Consumers may consent to a particular company using their biometric data for certain defined purposes, but still may not want them to share their information with others.

  While consumers can control the initial collection of their biometric by choosing the type of company they are doing business with, generally they will not be in a position to control what is done with it after it is collected. It is this potential for disclosure without consent that fuels the anxiety about biometrics.

  The notion of having some control over one's information is central to a sense of autonomy and self-determination. The issue of control, "lies at the very heart of the privacy concerns raised by this new technology. Individuals have an interest in determining how, when, why and to whom information about themselves, in the form of a biometric identifier, would be disclosed."[194]

  Unauthorized disclosure is the antithesis to personal control and informational privacy. A survey of Canadian consumers revealed that 83% strongly believed that their permission should be sought before an organization passed any information about them to another organization.[195]

Minimum Privacy Requirements

The privacy concerns associated with this technology have been recognized by the biometric industry, as a whole. In March 1999, the International Biometric Industry Association announced privacy principles[196] intended to encourage manufacturers, as well as organizations currently using or thinking about using biometrics, to adopt standards and procedures that will ensure biometric data are not misused.

However, it is essential to understand that, in the absence of data protection legislation for the private sector,[197] or specific legislation regulating the use of biometric identifiers, these nascent industry principles will not be sufficient to protect privacy.

As things presently stand, Canadian consumers need to represent their own interests regarding their biometric data. To do so, they need to be aware of both the benefits and concerns so they can make informed choices as to whether they wish to participate in consumer biometric applications.

With regard to the privacy-of-the-person issue, each individual must determine their own comfort level. The Supreme Court of Canada has recognized that the use of "a person's body without his consent to obtain information about him, invades an area of personal privacy essential to the maintenance of his human dignity."[198] However, it is very important to stress that participation in consumer biometric applications is *voluntary*. Companies cannot require consumers to give them their biometric data.

If privacy-of-the-person concerns arise from not understanding how the technology works, consumers should express their concerns and ask questions until they feel sufficiently familiar with the process to make an informed decision. However, if, in the final analysis, they continue to feel uncomfortable about giving their biometric — for whatever reason — they should not consent to its use.

Not every biometric application creates all the problems described earlier. Biometrics need not subvert informational privacy. A pro-privacy position should not be construed as anti-biometric.[199] The technology can actually be privacy enhancing if systems are designed with that objective in mind. "Indeed, the most effective means to counter technology's erosion of privacy is technology itself."[200] In a keynote address at a computer trade show in the fall of 1998, Bill Gates cited "online privacy problems as a key pitfall of a wired world" and stated that "biometrics offer a promising solution."[201]

Therein lies the paradox of biometrics: a threat to privacy in identifiable form, a protector of privacy in encrypted form; a technology of surveillance in identifiable form, a technology of privacy in encrypted form. Reliable forms of encryption can anonymize data and prevent unauthorized third parties from intercepting confidential information. In the case of biometrics, they can permit authentication without identification of the user.[202]

Privacy is not an absolute. For some people, the privacy threats outweigh any practical benefits they may receive from the use of biometrics. For others, while privacy concerns are significant, they can be effectively managed, allowing individuals to obtain the possible benefits offered by a biometric system. The informational privacy concerns discussed in this paper can be effectively addressed, even eliminated, if the use of biometric identifiers is done in accordance with fair information practices. These are internationally recognized standards designed to protect informational privacy. They form the basis of data protection schemes around the world, including Ontario's public sector freedom of information and protection of privacy legislation. Fair information practices also form the basis of the Canadian Standards Association *Model Code for the Protection of Personal Information*,[203] and a number of industry-specific privacy codes.

These practices are overlapping and cumulative principles that outline responsible information-handling practices designed to protect the privacy of the data subject. Adherence to all of the practices is necessary to achieve full informational privacy.

Below is a summary of the basic fair information practices,[204] as well as minimum standards that businesses should achieve prior to implementing a biometric system. Consumers should seek a business's compliance with these prior to consenting to the use of their biometric. These principles are applicable to all personal information, not just biometric data.

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.*

This principle is critical to protecting informational privacy. In many ways, it is a consumer's first line of defence. Informed consent is the "primary tool to protect privacy from technological invasion."[205] If a person knows about and consents to the collection of his or her biometric, that person is in a position to negotiate the terms of its use and disclosure.

There are a number of significant privacy protections subsumed under this principle — all of which consumers should seek out:

- Participation in a consumer biometric application should be strictly voluntary.
- Collection of biometric data should only be done with full and informed consent. Covert capture of biometric information in the context of a consumer application should not be permitted. No secret collections should exist.
- There should be no collection of the actual raw image of a biometric. Big Brother fears arise in the context of identifiable biometrics. For this reason, all consumer applications should be design so that the stored biometric template is only an encrypted, mathematical representation. This limitation on what is actually collected and retained is essential to ensure that biometric data cannot be used for any purpose other than identification.

- Quantitatively speaking, the use of a biometric can actually decrease the amount of personal information a company needs to accurately verify identity. As one author noted:

  > Paradoxically … it is when arguing in defence of privacy that the case for biometrics becomes the most compelling: the number of extra measures any organization needs to take to protect itself against fraud — or simply to do business efficiently and responsibly — is inversely proportional to the quality and reliability of the identification information it collects in the first place. Therefore, the more accurate that information is, the less likely the privacy of individuals will be violated in order to validate it.[206]

  Consumers should consider if they think it is necessary for a company collecting their biometric to have all the other personal information it may be requesting. For if the company has not collected personal information in the first place, it is not in a position to misuse it.

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.*

This is an essential corollary to the previous principle. Any biometric data held by a company must accurately identify the correct person. There must be no possibility of one person's biometric identifier being mistakenly linked to another or for that data to be altered. Once lost or compromised, a biometric trait can never be rehabilitated.

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.*

This means that the company should tell consumers why it wants their biometric *before* collecting it. Only by having this information will consumers be in a position to make an informed decision about whether they want to allow their biometric to be collected and used.

Businesses may claim that their actions are necessary to further the normal course of business,[207] but consumers must be able to decide what is appropriate for themselves. What may benefit the company is not necessarily synonymous with a consumer's privacy interests.

The most important point businesses should define for the consumer is whether their biometric will be used for a recognition or verification purpose. To date, consumer applications have been limited to verification applications. The next crucial aspect of any consumer biometric application that should be defined is whether the biometric will be used in an identifiable form:

> "… identification is not a necessity in every situation. Instead, verification suffices. In various situations it suffices to make sure that the person who actually makes use of a certain facility … is the same person as the one who is entitled to this facility. There is no need to know who precisely this person is. As long as the key factors of reliability and accountability are secure, identification of a person need not be necessary in various contexts."[208]

Given the reliability and accuracy of the process by which a biometric authentication credential is established, companies should give every consideration possible to designing their applications so that anonymous verification is possible.

Storing biometric identifiers off-line, such as in a secure smart card, offers significant privacy-enhancing capabilities. When stored in a database, biometric information is often connected to other personal data, such as names or addresses. This need not be the case with storage on a smart card. Here, the card could merely contain the biometric data. Such an arrangement means that no information may link the biometric data to a specific individual. This type of use allows for the verification of individuals, without the necessity of knowing the identity of the person (i.e., anonymous verification).[209] The use of biometrics at ATMs is an example of such an off-line application. Here the biometric technology aids in the verification of people, but does not require their identification.

Biometric encryption also may be used in a privacy-enhancing capacity to de-identify information contained in a database; that is, to anonymize the information by separating the identity of an individual from their sensitive information.

> The link between a person's identity and their information is the finger pattern which scrambles a computer pointer linking the two. This now places the individual in complete control of the information in his database.[210]

At a minimum, the company should clearly explain to consumers:

- How and why it is going to use the biometric data (i.e., the specific purposes for which the biometric is being collected, used, and disclosed).
- If anonymous verification will be possible, and if not, why not.
- The consequences of participating or not participating (i.e., risks and benefits), and what will happen if an individual subsequently chooses to leave the system after he or she has enrolled.

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, except:*

a) with the consent of the data subject, or

b) by the authority of law.

Following this principle automatically eliminates unauthorized use and disclosure privacy concerns. It would make the action taken by the fictitious insurance company, described earlier, unthinkable.

In order to implement this principle, consumers should insist that the company wishing to collect their biometrics has in place the proper technical and policy restrictions prohibiting:

- the use of biometric data for any reason other than verification of identity
- the sale, exchange, or provision of biometric data to third parties, except pursuant to a court order or warrant specifically authorizing it
- the identification of biometric data, even by the systems operator, using a means other than a match with a live biometric
- the discriminatory use of biometric data.

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

The use of biometrics may offer enhanced security for other data, but their sensitive and personal nature necessitates a high level of security for the biometric itself.

A biometric can itself be an effective security safeguard when it is controlled by its owners (e.g., to restrict access to their information by acting as an encryption key, or as an access control mechanism to secure a physical area or device containing their 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 over their own data.

Access to biometric data should be limited to only those within the company with a specific need to know. For example, frontline staff need not have access to the biometric data in order to confirm an individual as an authorized user. Also, storage of the biometric identifier with other client information may not be necessary. Depending upon the purpose of the application, storage of the biometric offline may be appropriate. A smart card could be used to store the biometric data, in a non-identified form, for use as an authentication credential, nothing more.

With smart, memory, or optical cards, there is a concern that if lost or stolen, someone could access the information. Encryption may be used to counter this concern. Using biometric encryption, the finger pattern could code a key that encrypts the data on the card. That key would not have to be securely stored. Also, only the individual with the finger pattern that coded the key could access the data on the card.

Biometric encryption uses the unique pattern in a person's fingerprint as his or her own private encryption or coding key. As an example, individual's fingerprints to code their PIN for accessing their bank machine. The coded PIN would have no connection to the finger

pattern. Stored in the database is only the coded PIN. The fingerprint pattern acts as the coding key of that PIN. The fingerprint pattern, encrypted or otherwise, is not stored anywhere during the process.[211]

Biometric encryption also may be used to scramble messages transmitted over the Internet. It provides security or confidentiality by virtue of encryption, authentication in that only the sender's finger pattern could have sent the information, and, in certain cases, non-repudiation since only the receiver's fingerprint pattern could have read it.[212]

Specific security safeguards for any biometric system should be that:

- the biometric data is stored separately from identifying information
- the stored biometric template cannot be re-engineered
- the stored biometric template is encrypted, particularly if it is to be transmitted over any network
- no evidence of the original biometric or raw data is retained after the template is created
- the system is designed to eliminate vulnerabilities to replay attacks
- all biometric data are destroyed in a secure manner when no longer necessary.

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.*

Not only does adherence to this principle mean that a company should not do anything with consumers' biometric data covertly, it also means it should be willing to tell its clients and the public about its policies and practices related to the biometric system.

The company should be able to tell consumers about any of their personal information that it holds, why it has the data, who is in charge of it (known as the data controller), and how it can be located should they wish to examine it. Basically, this is a requirement for the company to disclose its information handling and privacy protection practices.

Companies that want to introduce biometrics into their business practices have an obligation to communicate the benefits and privacy implications to all parties involved. Education should be an essential prerequisite to the introduction of any new technology because it enables users to make informed choices. In the context of biometrics, education helps to allay fears about privacy and enables users to become comfortable with the technology.

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

a) to obtain from a data controller, or otherwise, confirmation of whether or not the data controller has data relating to him or her

b) to have communicated to him data relating to him or her:

i) within a reasonable time

ii) at a charge, if any, that is not excessive

iii) in a reasonable manner

iv) in a form that is readily intelligible to him or her.

c) to be given reasons if a request made under subparagraphs (a) and (b) is denied, and to be able to challenge such denial

d) to challenge data related to him and, if the challenge is successful, to have the data erased, rectified, completed, or amended.

This is a necessary corollary to the openness principle. That principle defines a company's obligations to be transparent in its practices, while this principle gives consumers a specific right to ask questions and to challenge what the company is doing with their biometric.

Additionally, if designed with this objective in mind, a biometric system can permit the data subject to be an active participant with regard to controlling access to his or her own information, to safeguarding the integrity of that information, and to protecting against identity theft.

Even without this level of participation, in order to make an informed choice about biometrics consumers will need to understand why and how the system is being used, what their options are, and what benefits will follow. To properly weigh the pluses and minuses, they may wish to ask the company proposing the biometric system some detailed questions so they can determine if the company wanting to collect and use their biometric data is going to manage that information in a responsible manner, and in accordance with fair information practices, as outlined here.

If frontline staff are not sufficiently informed to answer their questions, consumers should ask to speak to someone who is in a position to provide the necessary answers. A recent Canadian survey assessed the level of awareness and knowledge of privacy laws and codes by frontline staff and how well they applied them when dealing with customers. The results indicated that, overall, employees of most organizations did quite poorly in their awareness and implementation of core privacy and data protection principles that applied to their place of employment.[213]

Consumers should make their inquiries prior to participating in a biometric identification scheme. Each biometric application will be different and each consumer will determine his or her own level of comfort. If a company is not receptive to potential customers' questions or responsive to their privacy and security concerns, then consumers should carefully consider whether they want to share their biometric data or, indeed, do any business with the company.

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

This principle gives effect to all the others. It means that the company, and more specifically, the data controller, should be held responsible for protecting biometric data. It is not sufficient for a company to say it will not invade consumer privacy or abuse biometric information. Before consumers consent to the collection of their biometric they should explore whether there is some type of mechanism for enforcing compliance with these practices.

Conclusion

Industry observers believe that the potential application of biometric technology is infinite. "Any situation that allows for an interaction between man and machine is capable of incorporating biometrics."[214] They also predict that the benefits of biometrics will make the technology's use, and consequently, its acceptance, inevitable.

Biometric technology in consumer applications is still remote in Canada. Accordingly, it is difficult to envisage the critical mass necessary for the technology to be considered "unavoidable," at this time. This may indeed change in the next decade.

Despite the very real benefits to both business and consumers, as outlined in this paper, the IPC believes that public acceptance of biometrics is not necessarily inevitable. It will only come if the privacy concerns associated with the technology are effectively addressed.

Whether biometrics are privacy's friend or foe is entirely dependent upon how the systems are designed and how the information is managed. While the biometric industry has made some positive initial steps, without private sector data protection legislation, Canadian companies are still free to use biometric data without restriction.

It must be recognized that the use of biometrics needs to "conform to the standards and expectations of a privacy-minded society."[215] The responsibility to ensure that this new technology does not knowingly or unknowingly compromise consumer privacy lies not only with businesses, but also with consumers.

Businesses must acknowledge and accept their obligation to protect their customers' privacy. Prior to introducing any biometric system, the impact that such an application may have on consumer privacy should be fully assessed. To appropriately and effectively balance the use of biometric information for legitimate business purposes with the consumer's right to privacy, companies should adopt and implement the fair information practices and requirements outlined in this paper. Voluntary adoption of such practices is essential if there is to be meaningful privacy protection of consumers' biometric data in the private sector.[216]

Consumers need to advocate for their own privacy rights.[217] They can make a difference by only doing business with companies that follow fair information practices and that make use of the privacy-enhancing aspects of biometrics in the design of their information management systems. Consumer preferences will be key in defining the appropriate uses and protection of biometrics. Consumers have the power — they need to use it wisely.

Notes

1. Martin J. Moylan, "Biometrics: Identifying Human Beings has Become a Multibillion dollar industry," *Hamilton Spectator*, December 29, 1997 p. B4.

2. Sari Kalin, "From Sci-Fi to Security: Biometrics Move Beyond Star Trek into Reality," *CIO Magazine*, April 15, 1998, <http://www.cio.com/archive/041598_et_content.html>, 04/17/98.

3. "The eyes have it: Bank machines to use iris scans?," *Toronto Sun*, December 1, 1997, p. 17.

4. Geoffrey Rowan, "Computers that recognize your smile," *Globe and Mail*, November 24, 1997, p. B3.

5. "Human Identity Reduced to a Bar Code," *Science Daily*, February 12, 1999, <http://www.sciencedaily.com/releases/1999/02/990212065653.htm>, 2/26/99.

6. "Big Brother biometrics: The identification you'll never leave home without," CNN fn Digital Jam, August 26, 1998, <http://japan.cnnfn.com/digitaljam/redherring/9808/26/redherring_biometrics/>, 12/29/98.

7. Gary Roethenbaugh, "Biometrics Explained," Section 1 — An Introduction to Biometrics and General History, <http://www.icsa.net/services/consortia/cbdc/sec1.shtml>, 12/29/98.

8. *The Shorter Oxford English Dictionary*, Editor, C. T. Onions (Oxford: Claredon Press, 1973), Volume II, p. 2420.

9. What a person *knows* (i.e., knowledge-based identification) and what a person *has* (i.e., token-based identification) are two authentication methods widely used to secure computer-based information systems. Biometrics (i.e., what a person *is or does*) offer a third method of authentication and security, as discussed in the Benefits section of this paper.

10. *The Concise Oxford Dictionary of Current English*, Eighth Edition, Editor, R.E. Allen (Oxford: Claredon Press, 1990), p. 73.

11. Gary Roethenbaugh, "ICSA Biometrics Buyer's Guide," Part 1 — Introduction, <http://www.icsa.net/services/consortia/cbdc/bg/introduction.shtml>, 12/29/98.

12. *Concise Oxford Dictionary*, p. 1002.

13. *Concise Oxford Dictionary*, p. 1363.

14. Roger Clarke, "Human Identification in Information Systems: Management Challenges and Public Policy Issues," *Information Technology & People*, Vol. 7, No. 4, December 1994, pp. 6–37, as cited in <http://www.anu.edu.au/people/Roger.Clarke/DV/HumanID>, 2/11/99.

15. George Tomko, "Biometrics as a Privacy-Enhancing Technology: Friend or Foe of Privacy?," Privacy Laws & Business 9th Privacy Commissioners'/Data Protection Authorities Workshop, Santiago de Compostela, Spain, September 15, 1998, <http://www.dss.state.ct.us/digital/tomko.htm>, 3/1/99.

16. Tomko, <http://www.dss.state.ct.us/digital/tomko.htm>, 3/1/99.

17. Corien Prins, "Biometric Technology Law: Making our body identify for us: Legal implications of biometric technology," *Computer Law & Security Report*, Vol. 14, No. 3, 1998, p. 160.

18. "Big Brother biometrics," CNN fn Digital Jam.

19. Roethenbaugh, "Biometrics Explained," Section 4 — Application Overview, <http://www.icsa.net/services/consortia/cbdc/sec4.shtml>, 12/29/98.

20. At the time of writing, the proposed biometric system is on hold, pending resolution of problems between Citibank Canada and the City of Toronto. Don Wanagas, "Welfare fingerprint proposal shelved," *National Post*, May 19, 1999, p. B2, and "Fingerprinting plan killed," *Toronto Star*, May 20, 1999, p. B2.

21. Guy Gugliotta, "Bar Codes for the Body make it to the Market: Biometrics May Alter Consumer Landscape," *Washington Post*, June 21, 1999, p. A1, <http://www.washingtonpost.com/wp-adv/archives/front.htm>, 9/7/99.

22. Roethenbaugh, "Biometrics Explained," Section 3 — Technology Overview, <http://www.icsa.net/services/consortia/cbdc/sec3.shtml>, 12/29/98.

23. IriScan Inc., "Spring Technologies and Jhoon Rhee Tae Kwon Do Launch New Technology that Enhances Customer Service," Press Release, <http://www.iriscan.com/html/springtech.html>, 5/5/99.

24. "Bank will ID its customers by pattern of eye's iris," May 13, 1999, <http://www.mercurycenter.com/resources/search/>, 9/7/99.

25. Paul Bobier, "Up close and personal: Biometrically identifying bank customers eye to eye is an invasion of privacy," *Kitchener-Waterloo Record*, p. A11.

26. Geoff Baker, "Newest form of ATM security catches eye of banking industry," *Ottawa Citizen*, July 3, 1997, p. C1.

27. Robert McKnight, "The Second Coming of Biometrics," *Canadian Security*, April/May 1998, p. 37.

28. International Biometric Group, "Overview of Biometrics — Face Geometry," <http://www.biometricgroup.com>, 8/13/99.

29. Association for Biometrics and International Computer Security Association, "1998 Glossary of Biometric Terms," as cited in Roethenbaugh, "ICSA Biometric Buyer's Guide," Appendix I, <http://www.iCSA.net/services/consortia/cbdc/bg/app1_glossary.shtml>, 8/13/99.

30. Philip E. Ross, "I can read your face," *Forbes*, December 19, 1994, pp. 304–305.

31. David Banisar, "Big Brother goes High-Tech," <http://www.worldmedia.com/caq/articles/brother.html>, 12/29/98.

32. *Biometric Technology Today*, September 1998, Volume 6, Number 5, pp. 6, 8.

33. "ATMs to use Face Recognition Technology," <http://www.networksusa.org/fingerprint/page5a/fp-atm-facial-scans.html>, 4/22/99.

34. John Burnell, "Identifying the biometric opportunity," *Automatic ID News*, <http://www.autoidnews.com/technologies/concepts/affordbl.htm>, 4/26/99.

35. Laurent Belsie, "Coming Soon: ATMs That Recognize Your Eyes," *Christian Science Monitor*, December 2, 1997.

36. Vince Beiser, "Casinos Fight Back with Tech," *Wired News*, May 4, 1999, <http://www.wired.com/news/news/technology/story/19463.html>, 6/15/99.

37. One such system attempts to categorize faces according to the degree of fit with a set of "eigenfaces." It has been postulated that every face can be assigned a "degree of fit" to each of 150 eigenfaces. In addition, the contention is that only the template eigenfaces with the 40 highest "degree of fit" scores are necessary to reconstruct a face with over 99% accuracy. This method uses computer-based analysis of digital images of actual photographs of individuals. Thomas Ruggles, "Comparison of Biometric Techniques," The Biometric Consulting Group, last revision March 15, 1998, <http://biometric-consulting.com/bio.htm>, 7/19/99.

38. Lawrence Surtees, "Your Secret Identity: The spread of biometric technology means that your fingertips, hands, eyes and face have become physical passwords that can unlock doors and grant you access to computer terminals, bank machines and even Disney World," *Globe and Mail*, December 10, 1998, p. C1, and at <http://www.globetechnology.com/gam/News/19981210/TWBIOM.html>, 5/12/99.

39. Association for Biometrics and Internationals Computer Security Association, "1998 Glossary of Biometric Terms."

40. "Fingerprint children for free," *Toronto Star*, September 10, 1998, p. B2.

41. "Bank of America Offers Fingerprint Access to Online Banking," January 6, 1999, Press Release, <http://www.internetnews.com/ec-news/1999/01/0601-bank.html>, and Bank of America News, <http://www.biometricgroup.com/news_boa.htm>, 5/5/99.

42. Tom Godfrey, "Banks eye taking cheque thumbprint," *Toronto Sun*, April 27, 1998, p. 26.

43. Kalpana Sprinivasan, "American firms give thumbs-up to security system," *Toronto Star*, April 22, 1998, p. A2.

44. *The Biometric Digest*, <http://webusers.anet-stl.com/~wrogers/biometrics/>, 5/14/99.

45. Simon G. Davies, "Touching Big Brother: How biometric technology will fuse flesh and machine," *Information Technology & People*, Vol. 7, No. 4, 1994, <http://www.interlog.com/~cjazz/biometric.htm>, 12/29/98.

46. Bill Wilson, "Hand geometry boasts simplicity, convenience," *Access Control*, March 1992, Reprint, p. 1.

47. Susannah Kilroy, "Biometric Identification and Access Control Go Hand-In-hand," *SP&I News*, April 1998.

48. Kilroy, April 1998.

49. George Tomko, "Biometric Encryption — New Developments in Biometrics," The 18th International Privacy and Data Conference, September 19, 1996, at <http://infoweb.magi.com/~privcan/conf96/se_tomko.html>, 4/21/99.

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

51. Recognition System, "A Show of Hands Keeps School Children Safe," Press Release, November, 16, 1998, <http://www.recogsys.com/rsi_public_html/press.html>, 5/5/99.

52. Surtees, "Your Secret Identity."

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

54. Roethenbaugh, "Biometrics Explained," Section 3 — Technology Overview.

55. BioMet Partners, Inc., "New 3D Finger Geometry Biometrics For OEM's and Systems Integrators," Press Release, January 15, 1999, <http:www.biomet.ch/press.htm>, 5/5/99.

56. Roethenbaugh, "ICSA Biometrics Buyer's Guide," Chapter 4 — Types of Biometric, <http://www.iCSA.net/services/consortia/cbdc/bg/chap4.shtml>, 12/29/99.

57. F. James, "Body scans could make ID process truly personal," *Chicago Tribune*, June 4, 1997, as cited in John D. Woodward, "Biometrics: Privacy's Foe or Privacy's Friend?," *Proceedings of the IEEE*, Vol. 85. No. 9, September 1997, p. 1483.

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

59. Association for Biometrics and International Computer Security Association, "1998 Glossary of Biometric Terms."

60. Roethenbaugh, "ICSA Biometrics Buyer's Guide," Chapter 4 — Types of Biometrics.

61. Baker, "Newest form of ATM security."

62. SAFLINK Coporation, "Home Shopping Network and SAFLINK Corporation Ship Biometric Security to 5,000 Families," Press Release, May 11, 1999, <http://biz.yahoo.com/prnews/990511/fl_saflink_1.html>, 5/12/99.

63. SAFLINK Corporation, "SAFLINK Develops Way to Secure Internet Banking/Brokerage Account Balances, Bill Payment, and Funds Transfer Using Biometrics," Press Release, June 24, 1999, <http://biz.yahoo.com/prnews/990624/fl_saflink_1.html>, 6/24/99.

64. George Cole, "Giving Voice to Security," *Financial Times*, September 15, 1995, <http://www.weverify.com/vervcsec.htm>, n.d.

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

66. International Biometric Group, "Overview of Biometrics — Keystroke Dynamics," <http://www.biometricgroup.com/a_bio1/technology/cat_keystroke.htm>, 4/22/99.

67. Roethenbaugh, "Biometrics Explained," Section 3 — Technology Overview.

68. Matthew Nelson, "Net Nanny Finds New Keys to Security: Let you fingers do the walking to a new form of password protection," *PC World*, October 9, 1998, <http://www.pcworld.com/cgi-bin/pcwtoday?ID_8361>, 10/13/98.

69. Net Nanny, "Net Nanny Releases Much Anticipated Alpha Version of BioPassword, its Patented Keystroke Dynamics Security Solution," Press Release, August 27, 1998, <http://biz.yahoo.com/bw/980827/Net_nanny_1.html>, 8/28/98.

70. Roethenbaugh, "Biometrics Explained," Section 3 — Technology Overview.

71. Roethenbaugh, Section 3 — Technology Overview.

72. Association for Biometrics and International Computer Security Association, "1998 Glossary of Biometric Terms."

73. "Pinched by the ear," *Toronto Star*, July 6, 1995, p. 43.

74. Laura Lyne McMurchie, "Identifying risks in biometrics use," *Computing Canada*, February 12, 1999, p. 12.

75. Roethenbaugh, "Biometrics Explained," Section 3 — Technology Overview.

76. Laura Spinney, "Crooks smelly armpits give the game away," *New Scientist*, September 14, 1994, p. 10.

77. Association for Biometrics and International Computer Security Association, "1998 Glossary of Biometric Terms."

78. Roethenbaugh, "Biometric Explained," Section 3 — Technology Overview.

79. Richard Foot, "Two pathologists want airlines to keep DNA records," *National Post*, December 29, 1998, p. A5.

80. "DNA Samples Taken from Newborns in Florida," *National Post*, January 28, 1999, p. A13.

81. Frost & Sullivan, "Biometrics to Guard Against Fraud: Identification Security on the Horizon," October 14, 1997, <http://www.networkusa.org/fingerprint/page5a/fp-atm-facial-scans.html>, 4/22/99.

82. "Moving Beyond Passwords: Biometrics to Introduce Retina Scans, Voices, Prints," ABCNews.com, November 18, 1998, <http://abcnews.go.com/sections/tech/DailyNews/net_security981118.html>, 4/21/99.

83. Surtees, "Your Secret Identity."

84. Integrated Telecommunications Systems, "For Canadian Companies."

85. "Moving Beyond Passwords."

86. "Reading the future of the technologies that read you," Reprinted from the December 1998 issue of *Automatic I.D. News*, <http://www.autoidnews.com/1298/1298biomet.html>, 12/1/98.

87. Burnell, "Identifying the biometric opportunity."

88. Ashley Dunn, "PC security in the blink of an eye: The evolution of biometrics has started to make its pressure felt in the corporate and personal computer worlds with high-tech, low-cost identification systems," *National Post*, December 10, 1998, p. C16.

89. Kalin, "From Sci-Fi to Security."

90. Carey Heckman, "Gateways to the Global Market: Consumers and Electronic Commerce," <http://www-techlaw.stanford.edu/pages/OECDBack.html>, 4/23/99.

91. Roethenbaugh, "ICSA Biometrics Buyer's Guide," Chapter 3 — The Need for Biometrics, <http://www.icsa.net/services/consortia/cbdc/bg/chap3.shtml>, 4/28/99.

92. TrueFace Financial Solutions, "Enhancing Customer Service and Reducing Fraud," <http://www.miros.com/Financial.htm>, 5/6/99.

93. Clarke, "Human Identification."

94. Canadian Bankers Association, "Electronic Banking Fast Facts," November 1998, <http://www.cba.ca/eng/Statistics/FastFacts/abms.htm>, 11/25/98.

95. LGS Group Inc., "ECommerce and Security in Canada: The Consumer Perspective," <http://www.lgs.com/Services/Serv_Information_Highway.htm>, 5/6/99.

96. Roethenbaugh, "Biometrics Explained," Section 4 — Application Overview.

97. Association for Biometrics, "A Five Step Guide to Selecting a Biometric System," <http://www.afb.org.uk/public/5steps.html>, 4/21/99.

98. Heckman, "Gateways to the Global Market."

99. Kevin S. McCurley, "Biometric User Authentication vs. Data Authentication," <http://www.cs.sandia.gov/~mccurley/health/node15.html>, 4/21/99.

100. Dale Anne Freed, "Warning sounded on credit card fraud," *Toronto Star*, May 31, 1999, p. A1.

101. Craig Bicknell, "Credit Card Fraud Bedevils Web," *Wired News*, <http://www.wired.com/news/print_version/email/explode-infobeat/business/story/18904.html?wnpg=all>, 4/16/99.

102. "Poll: Online shoppers sweat credit card fraud," *Arkansas Online*, May 20, 1999, <http://www.ardemgaz.com/today/biz/debcardfraud20.html>, 5/20/99.

103. Ekos Research Associates, Inc., "Information Highway and the Canadian Communications Household Survey," Press Release, February 23, 1998, <http://www.ekos.com/FEB98/HTM>, 3/8/99.

104. Surtees, "Your Secret Identity."

105. Amitai Etzioni, *The Limits of Privacy*, New York: Basic Books, 1999, p. 109.

106. U.S. Public Interest Research Group, "Theft of Identity: The Consumer X-Files," August 1996, p. 14.

107. Mari Frank and Beth Givens, *Privacy Piracy: A Guide to Protecting Yourself from Identity Theft*, Office Depot: Spring 1999, p. 1.

108. For more information on identity theft see "Identity Theft: Who's Using Your Name?," June 1997, and "If you wanted to know… Identity Theft and Your Credit Report: What You Should Do to Protect Yourself," which are available from the Office of the Information and Privacy Commissioner/Ontario at the address indicated on the inside cover of this paper, or from the agency's website at: <www.ipc.on.ca>.

109. e-DENTIFICATION Inc., "Three Companies Join Forces to Offer the First Genuine Privacy Protection for Electronic Commerce and Communications," Press Release, July 19, 1999, <http://biz.yahoo.com/prnews/990719/pa_e_denti_1.html>, 7/21/99.

110. "Tornadoes pose ID problems," *Globe and Mail*, May 12, 1999, p. B25, and "Storm Victims Re-Establish Identity," *Guardian Online*, May 12, 1999, <http://www.newsunlimited.co.uk/Breaking_News/US/0,3560,260702,00.html>, 5/20/99.

111. "The Fourth Annual Computer Security Institute Survey," <http://LegalNews.FindLaw.com/Intellectual_Property.html>, 3/12/99.

112. "Moving Beyond Passwords."

113. Sylvia Dennis, "Passwords offer limited protection, says study," *Computer Canada*, February 12, 1999, p. 12.

114. Roethenbaugh, "ICSA Biometrics Buyer's Guide," Chapter 3 — The Need for Biometrics.

115. Department of Computer Science and Engineering, Michigan State University, "An Overview of Biometrics, Pattern Recognition and Image Processing Lab," <http://biometrics.cse.msu.edu/info.html>, 2/4/99.

116. Roethenbaugh, "ICSA Biometrics Buyer's Guide," Chapter 3 — The Need for Biometrics.

117. Thomas L. Norman, "Selling Biometrics," *Canadian Security*, April/May 1998, p. 1.

118. Roethenbaugh, "ICSA Biometrics Buyer's Guide," Chapter 2 — How Biometrics Work, <http://www.icsa.net/services/consortia/cbdc/bg/chap2.shtml>, 4/28/99.

119. Francis Declerq, "Biometrics help maintain security," *Computing Canada*, May 14, 1999, p. 29.

120. Biometric encryption uses two-dimensional information in a finger pattern to scamble the information into a unique pattern known as a Bioscrypt (a compound of a biometric and encryption). The finger pattern, which acts as the scrambling key, is not stored anywhere during the process. Only the Bioscrypt is stored and it is considered to be irreversible without the live finger pattern. The Bioscrypt can only be uncoded by the correct live finger pattern. Tomko, "Biometric Encryption."

121. Tomko, "Biometrics as a Privacy-Enhancing Technology."

122. Gary Gunnerson, "Are you Ready for Biometrics?," *ZDNet*, February 8, 1999, <http://www.zdnet.com/pcmag/stories/reviews/0,6755,386987,00.html>, 6/15/99.

123. Norman, "Selling Biometrics," p. 41.

124. Prins, "Biometric Technology Law," p. 160.

125. See: Biometric Group, "Zephyr Analysis," <http://www.biometricgroup.com/a_biometric_0/zephyr.htm>, 7/20/99; Roethenbaugh, "Biometrics Explained," Section 3 — Technology Overview; Norman, "Selling Biometrics," p. 44; and Kalin, "From Sci-Fi to Security."

126. Rosen, "Biometric Systems Open the Door," p. 59.

127. Roethenbaugh, "Biometrics Explained," Section 2 — How Biometrics Work, <http://www.icsa.net/services/consortia/cbdc/sec2.shtml>, 11/16/98.

128. McCurley, "Biometric User Authentication."

129. Donald R. Richards, "Rules of Thumb for Biometric Systems," *Security Management*, October 1995, p. 67.

130. Roethenbaugh, "Biometrics Explained," Section 5 — Truths And Myths, <http://www.icsa.net/services/consortia/cbdc/sec5.shtml>, 7/19/99.

131. Roethenbaugh, "Biometrics Explained," Section 2 — How Biometrics Work.

132. The results of one such study may be found in *ComputerWorld Canada*, December 19, 1997, p. 33.

133. There have been a few studies of public attitudes toward biometric systems. See Alan F. Westin, "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, <http://www.nrid.com/privacy.html>, 2/3/97; and J. Holmes, L. Wright, R. Maxwell, Sandia National Laboratories, "A Performance Evaluation of Biometric Identification Devices," SAND91-0278/UC-906, June 1997, as cited in Ruggles, "Comparison of Biometric Techniques."

134. Roethenbaugh, "Biometrics Explained," Section 5 — Truths And Myths.

135. Anil K. Jain, Lin Hong, Sharath Pankanti, and Ruud Bolle, "An Identity-Authentication System Using Fingerprints," *Proceedings of the IEEE*, Vol. 85, No. 9, September 1997, p. 1366.

136. Ruggles, "Comparison of Biometric Techniques."

137. Holmes, Wright, Maxwell, "A Performance Evaluation of Biometric Identification Devices," as cited in Ruggles, "Comparison of Biometric Techniques."

138. Gerald Lazar, "Agencies Scan Biometrics for Potential Applications," *Federal Computer Week*, January 20, 1997, as cited in Sean M. O'Connor, "Collected, Tagged, and Archived: Legal Issues in the Burgeoning Use of Biometrics for Personal Identification," <http://lummi.stanford.edu/class/law495/WWW/oconnor.htm>, 2/11/99.

139. Richards, "Rules of Thumb for Biometric Systems," p. 71.

140. Richards, p. 71.

141. Ruggles, "Comparison of Biometric Techniques."

142. Ruggles.

143. O'Connor, "Collected, Tagged, and Archived," and Roethenbaugh, "Biometrics Explained," Section 5 — Truths And Myths.

144. Ken Philips, "Biometric Identification Looms on Landscape of Network Log-Ins: High-End Technology is Becoming More Affordable," *PC WEEK*, March 26, 1997, as cited in O'Connor, "Collected, Tagged, and Archived."

145. J.P. Campbell, L.A. Alyea, and J.S. Dunn, "Biometric security: Government applications and operations," 1996, as cited in Jain, Hong, Pankanti, and Bolle, "An Identity-Authentication System Using Fingerprints," p. 1367.

146. Roethenbaugh, "ICSA Biometric Buyer's Guide," Chapter 5 — Biometric Standards & Testing, <http://www.icsa.net/services/consortia/cbdc/bg.chap5.shtml>, 4/28/98.

147. Tomko, "Biometrics as a Privacy-Enhancing Technology."

148. Moylan, "Multibillion dollar industry," p. B4.

149. Association for Biometrics and International Computer Security Association, "1998 Glossary of Biometric Terms."

150. Vein Biometric Home Page, <http://innotts.co.uk/~joerice/>, 4/26/99.

151. Jain, Hong, Pankanti, and Bolle, "An Identity-Authentication System Using Fingerprints," p. 1366.

152. "Biometric Security," *PC Magazine Online*, <http://www.zdnet.com/pcmag/features/biometrics/bench.html>, and <http://www.zdnet.com/pcmag/features/biometrics/break.html>, 2/22/99.

153. Bruce Schneier, "Biometrics: Truth and Fictions," *Crypto-Gram*, August 15, 1998, <http://www.counterpane.com/crypto-gram-9808.html#biometrics>, 7/20/99.

154. Peter Wayner, "Signing On with Your Fingerprints," *New York Times*, March 19, 1999, p. G11.

155. Peter Wayner, *New York Times*, October 29, 1997, as cited in Tomko, "Biometrics as a Privacy-Enhancing Technology."

156. Tomko, "Biometrics as a Privacy-Enhancing Technology."

157. Larry Lang, "APIs reach out and touch human-ID systems," *CMP Net*, February 9, 1998, <http://www.techweb.com/se/directlink.cgi?EET19980209S0021>, 4/26/99.

158. Schneier, "Biometrics: Truth and Fictions."

159. Wayner, "Signing On with Your Fingerprints."

160. Moylan, "Multibillion dollar industry," p. B4.

161. Wayner as cited in Tomko, "Biometrics as a Privacy-Enhancing Technology."

162. Tomko, "Biometrics as a Privacy-Enhancing Technology."

163. Moylan, "Multibillion dollar industry," p. B4.

164. R. v. Dyment (1988), 55 D.L.R. (4th) 503 at 513 (S.C.C.).

165. House of Commons Standing Committee on Human Rights and the Status of Persons with Disabilities, *Privacy: Where do we draw the line? Report of the House of Commons Standing Committee on Human Rights and the Status of Persons with Disabilities*, Ottawa: Public Works and Government Services Canada, April 1997, p. 6.

166. Department of Communications and Department of Justice, *Privacy and Computers*, Ottawa: Information Canada, 1972, as cited by the Commission on Freedom of Information and Individual Privacy, *Public Government for Private People: The Report of the Commissioner on Freedom of Information and Individual Privacy/ 1980*, Toronto: Ministry of Government Services, 1980, Vol. 3, p. 499.

167. Clarke, "Human Identification."

168. Clarke.

169. Norman, "Selling Biometrics," p. 42.

170. Roethenbaugh, "Biometrics Explained," Section 5 — Truths and Myths.

171. "IBIA Announces Privacy Principles," *Biometrics in Human Services User Group*, Volume 3, Issue 3, June 1999, <http://www.dss.state.ct.us/digital/news14/bhsug14.html>, 5/19/99.

172. Clarke, "Human Identification."

173. Westin, "Public Attitudes Toward the Use of Finger Imaging Technology."

174. "Finger-pointer," *Toronto Star*, May 22, 1997, p. A7; see also Laurie Monsebraaten, "Report banks fingerprint ID for welfare: Metro again to consider scheme," *Toronto Star*, May 2, 1997, p. A3.

175. "Biometrics," *Globe and Mail*, December 17, 1998, <http://news.globetechnology.com>, 5/12/99.

176. Davies, "Touching Big Brother."

177. The results of a 1992 survey of Canadian households by Ekos Research Associates Inc. showed that:

- 60% of respondents said they had less privacy than they did a decade ago;
- 40% felt strongly their privacy had eroded
- 80% felt computers had reduced privacy
- 54% were extremely concerned about linking personal information from one electronic database to another
- 72% felt being in control of who gets information about them is extremely important
- 67% felt controlling what information is collected about them is extremely important.

Privacy Revealed: The Canadian Privacy Survey as cited in Paul Bobier, "Privacy at Risk," *Government Computer*, February 1998, p. 16.

178. M.G. Stone and Malcolm Warner, "Power, Privacy and Computers," *The Political Quarterly*, Vol. 40(1969), p. 260, as cited in Colin J. Bennett, *Regulating Privacy: Data Protection and Public Policy in Europe and the United States*, Ithaca: Cornell University Press, 1992, p. 29.

179. Robert Moskowitz, "Are biometrics too good?," *Networking Computing*, January 25, 1999, p. 85, <http://www.infowar.com/class_1/99/class1_0125991_j.shtml>, 4/22/99.

180. O'Connor, "Collected, Tagged, and Archived."

181. Moskowitz, "Are biometrics too good?"

182. O'Connor, "Collected, Tagged, and Archived."

183. Roethenbaugh, "Biometrics Explained," Section 5 — Truths and Myths.

184. Deborah G. Johnson, *Computer Ethics*, Englewood Cliffs, N.J.: Prentice-Hall, 1985, p. 66, as cited in James H. Moor, "How to Invade and Protect Privacy with Computers," *The Information Web: Ethical and Social Implications of Computer Networking*, edited by Carol C. Gould, San Francisco: Westview Press, Inc., 1989 pp. 60–61.

185. KPMG LLP and Indiana University, "IU/KPMG Study Reveals that Consumers are Wary about how Retailers Obtain and use Information about them," Press Release, May 24, 1999, <http://biz.yahoo.com/prnews/990524/fl_kpmg_st_1.html>, 5/31/99.

186. Arthur R. Miller, *The Assault on Privacy: Computers, Data Banks, and Dossiers*, Ann Arbor: University of Michigan Press, 1971, p. 21, as cited in Bennett, *Regulating Privacy*, p. 29.

187. Woodward, "Biometrics: Privacy's Foe or Privacy's Friend?," p. 1484.

188. James Laban, "Privacy Issues Surrounding Personal Identification Systems," April 1996, p. 3 of 29, <http://www.dss.state.ct.us/index.html>, 8/26/99.

189. Ann Cavoukian, "Privacy and Biometrics: An Oxymoron or Time to take a 2nd look?" Computers, Freedom and Privacy Conference 1998, Austin, Texas, <www.ipc.on.ca/web_site.eng/matters/sum_pap/papers/cfp98.htm>, 24/5/99.

190. Kenneth P. Nuger, "Biometric Applications: Legal and Societal Considerations," San Jose State University, <http://www.engr.sjsu.edu/~graduate/biometrics/privatei.html>, 4/26/99.

191. Roethenbaugh, "Biometrics Explained," Section 5 — Truths and Myths.

192. H. Chen, *Medical Genetics Handbook*, St. Louis, MO: W.H. Green, pp. 221–226, and M. Skole, "Finger and palm prints: A window on your health," *Glamour*, pp. 248–250, April 1984, as cited in Woodward, "Biometrics: Privacy's Foe or Privacy's Friend?," p. 1484.

193. B. Bates, *A Guide to Physical Examination and History Taking*, 5th ed., Philadelphia, PA: Lippincott, 1991, pp. 181–215, and Interview with F.P. Nasrallah and A.S. DiDo, Washington, D.C., April 4, 1994, as cited in Woodward, "Biometrics: Privacy's Foe or Privacy's Friend?," pp. 1484–1485.

194. Woodward, "Biometrics: Privacy's Foe or Privacy's Friend?," p. 1483.

195. Ekos Research Associates Inc., *Privacy Revealed: The Canadian Privacy Survey*, (Ottawa: 1993), p, 11.

196. The International Biometric Industry Association (IBIA) was formed in September 1998 and is open to all biometric manufacturers, integrators, and end users who "agree to honor a code of ethics that recognizes the protection of personal privacy as a fundamental obligation of the biometric industry." The IBIA principles are:

    1. Biometric data is electronic code that is separate and distinct from personal information, and provides an effective, secure barrier against unauthorized access to personal information. Beyond this inherent protection, IBIA recommends safeguards to ensure that biometric data is not misused to compromise any information, or released without personal consent or the authority of law.

2. In the private sector, IBIA advocates the development of policies that clearly set forth how biometric data will be collected, stored, accessed, and used, and that preserve the rights of individuals to limit the distribution of the data beyond the stated purposes.

3. In the public sector, IBIA believes that clear legal standards should be developed to carefully define and limit the conditions under which agencies of national security and law enforcement may acquire, access, store, and use biometric data.

4. In both the public and private sectors, IBIA advocates the adoption of appropriate managerial and technical controls to protect the confidentiality and integrity of databases containing biometric data.

"IBIA Announces Privacy Principles: Biometric Industry Group Recommends Measures to Protect Personal Information," Press Release, March 24, 1999, <http://www.iriscan.com/privacy.htm>, 5/12/99.

197. At the 18th International Conference on Privacy and Data Protection, held in Ottawa in September 1996, the Minister of Justice announced the Canadian federal government's commitment to have "federal legislation on the books that will provide effective, enforceable protection of privacy rights in the private sector" by the year 2000. At the time of publication, it can be reported that the *Personal Information Protection and Electronic Document Act* (Bill C-54) had been introduced into the House of Commons and was being debated when the House rose for the Summer. It is anticipated that consideration of the Bill will resume when the House returns in the Fall of 1999.

198. R. v. Dyment [1988] 2 S.C.R. 417 at 431–32, as cited in Privacy Commissioner of Canada, *Drug Testing and Privacy*, Ottawa: Minister of Supply and Services Canada, 1990, p. 18.

199. Testimony of John D. Woodward, Jr. for 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, <http://www.dss.state.ct.us/digital/legal1.htm>, 4/22/99.

200. Remarks by Chairman Alan Greenspan, Federal Reserve Board, Conference on Privacy in the Information Age, Salt Lake City, Utah, March 7, 1997, <http://federalreserve.gov/boarddocs/speeches/1997/19970307.htm>, 5/27/99.

201. "More than passwords needed for Internet privacy," *Findlaw Legal News*, <http://LegalNews.FindLaw.com/scripts/legal/19981210/bcinternetsecurity.html&frame_right>, 12/11/98.

202. Ann Cavoukian, "Go Beyond Security — Build in Privacy: One Does Not Equal the Other," CardTech/SecurTech '96 Conference, Atlanta, Georgia, May 1996, <http://www.eff.org/pub/Crypto/960514_cavoukian_priv-sec.speech>, 7/21/99.

203. The Model Code, as well as the publications related to its implementation, are available at: <http://www.csa.ca/english/product_services/index_info.htm>, 5/14/99, or from 178 Rexdale Boulevard, Etobicoke, Ontario, Canada, M9W 1R3.

204. These fair information practices are based on the "Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data" established by the Organization for Economic Co-operation and Development (OECD) in September 1980. Canada adopted the guidelines in 1984. A complete text of the OECD Guidelines is provided in Wayne Madsen, *Handbook of Personal Data Protection*, New York: Stockton Press, 1992, pp. 992–996.

205. Standing Committee on Human Rights and the Status of Persons with Disabilities, *Privacy: Where do we draw the line?*, p. 11.

206. Marc C. Duez, "Biometrics Meet Privacy: The Forces at Play," 1997, p. 21.

207. Nuger, "Biometric Applications: Legal and Societal Considerations."

208. Prins, "Biometric Technology Law," p. 163.

209. Prins, 162–163.

210. Tomko, "Biometric Encryption."

211. Tomko, "Biometrics as a Privacy-Enhancing Technology."

212. Tomko, "Biometric Encryption."

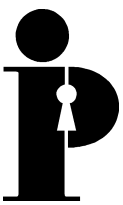
213. Consumer Awareness Network and Public Interest Advocacy Centre, "The 1998 Personal Data Protection and Privacy Review," May 1999. See also, Tracy LeMay, "Consumer privacy still minor issue — survey," *National Post*, May 26, 1999, p. D1.

214. Roethenbaugh, "ICSA Biometrics Buyer's Guide," Chapter 3 — The Need for Biometrics.

215. Davies, "Touching Big Brother."

216. For more information about how businesses can protect consumer privacy, see "Privacy Protection Makes Good Business Sense," October 1994, which is available from the Office of the Information and Privacy Commissioner/Ontario at the address indicated on the inside cover of this paper, or from the agency's website at: <www.ipc.on.ca>.

217. For more information on consumer privacy, see "Privacy Alert: A Consumer's Guide to Privacy in the Marketplace," May 1994, which is available from the Office of the Information and Privacy Commissioner/Ontario at the location indicated in the inside cover of this paper or from the agency's website at: <www.ipc.on.ca>.



Information and Privacy Commissioner/Ontario

2 Bloor Street East
Suite 1400
Toronto, Ontario
M4W 1A8

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