20/20

ACCESS & PRIVACY EXCELLENCE... 20 YEARS IN THE MAKING

20th Anniversary Collection

Ann Cavoukian, Ph.D.

INFORMATION AND PRIVACY COMMISSIONER OF ONTARIO

Ann Cavoukian, Ph.D.
Information and Privacy Commissioner of Ontario

Introduction

So much has changed since the late-1980s when my attention was first captured by freedom of information and protection of privacy.

In the early -80s, I was working as the head of the Research Services Department at the Office of the Attorney General of Ontario. The Honourable Justice Sidney Linden was breaking new ground as Ontario's first Public Complaints Commissioner, conducting independent reviews of complaints against the police. In 1987, he was appointed Ontario's first Information and Privacy Commissioner (IPC). When he asked me to join him as the first Director of Compliance, I was delighted to accept.

The rest, as they say, is history. On January 1, 2008, the IPC will mark its 20th anniversary. It's been an honour and a privilege to be part of this organization, since its inception. I'm very proud of the work we've done over the years.

This anthology celebrates not only our 20th anniversary, but also some of the most critical and groundbreaking moments in access and privacy that we've seen in our 20-year history.

I have served as Commissioner for 10 of the past 20 years. In that time, I've seen many important changes.

In the area of freedom of information, I've watched as democracies around the world have recognized that citizens have the right to know what their government is doing, and to hold it responsible for its actions. In our own province, I've seen a growing understanding that reactive access processes are not the only hallmark of an open and transparent government. It's been gratifying to help governments move beyond mere compliance toward embracing routine disclosure and active dissemination as key elements of transparent and fully accountable public administration.

The world of privacy has changed even more dramatically over the years. The very concept of privacy has evolved over the past two decades, spurred on by the information technology revolution, the explosion of the world wide web, and, more recently, the events of September 11, 2001.

In the early days of the IPC, surveillance cameras were not yet ubiquitous features in urban landscapes. Biometric passports were still the stuff of science fiction movies. Radio Frequency Identification (RFID) tags were limited to military applications. And identity theft, for the most part, was limited to dumpster diving and forged drivers' licenses.

Today, surveillance cameras are being implemented with increasing frequency. Several countries around the world are using biometric passports. Item-level RFID tags on consumer products have become a source of contentious debate. And identity theft has become the fastest-growing form of consumer fraud in North America.

What's more, countless databases around the world now hold an unimaginable amount of personal information about all of us, and of an increasingly granular nature. And in today's world, records can be easily copied, duplicated, stored and transmitted with minimal accountability and few safeguards.

All of this has raised and continues to raise some very legitimate and important questions. If I apply for a biometric passport, can I be sure that my information will not be used beyond its specified purpose or fall into the wrong hands? If I buy a consumer item with an RFID tag, will the company be able to track me? If I do my banking online, how can I be sure that I am at a legitimate site and not being driven by identity thieves?

These are the types of questions that have been emerging for the past two decades as a result of both dramatic and incremental technological changes. In the post-September 11th world, such questions have taken on a new kind of urgency as the world struggles to regain a sense of security.

Without question, the growth of terrorism is of concern to most people. As Commissioner, however, I also fear the potential loss of our rights and freedoms, including the right to privacy. Shortly after September 11th, I wrote a commentary, entitled *Public Safety is Paramount, but Balanced Against Privacy,* for the CBC's website, at the request of the CBC. In this, and in speeches and interviews that followed, I took the position that while

we must certainly protect the safety of the public, we must also ensure that new security measures introduced are both effective and necessary. Most importantly new security measures must be real, not illusory. In my view, it would be untenable to give up our privacy and our freedom simply for the *appearance* of security. Losing our freedom to gain a false sense of security is clearly not a tradeoff worth making.

And privacy is fundamental to freedom. Without privacy, there would be little to distinguish our nation from a police state. In the words of Benjamin Franklin, "Those who would give up essential liberty to purchase a little temporary safety, deserve neither liberty nor safety."

No matter how complex the situation seems, or how muddied the waters become, my belief has long been that concerns about the protection of our personal information can be addressed in two ways. One is to use information technology to our advantage, and the other is to urge the organizations entrusted with our personal information to embed a culture of privacy.

Technology itself is not inherently a threat to privacy. Indeed, technology can both threaten and enhance privacy. The key lies in how it is used.

Back in 1995, I co-authored a paper with the Netherlands Data Protection Authority on privacy-enhancing technologies called *Privacy-Enhancing Technologies: The Path to Anonymity*. The paper argued that while legal instruments are useful in protecting privacy, they are not enough. We must enlist the support of technology to best protect privacy. "Privacy by design" has become our mantra.

Today, as technological innovations continue to pose new threats to privacy, my view continues to be that the use of privacy-enhancing technologies to minimize those threats is critical for maintaining the right to privacy now and in the future. Privacy-enhancing technologies are available and ready for deployment; what is needed is simply the will to implement them.

This "will" is an important aspect of what I call a "culture of privacy." All organizations that handle personal information need to develop and nurture a mindset that reflects a commitment to better information management and privacy protection. Privacy policies must be woven into the fabric of day-to-day operations and communicated clearly to employees – because even the most advanced technology and the most rigorous privacy policies cannot be successful in the absence of a supportive organizational culture.

Fostering the development of such a culture in the public, private, and health care sectors is an important aspect of my mandate as Commissioner. That's why my Office has taken such an active role in public education and heightened awareness. The papers published here reflect some of the most important issues we've addressed in the past 20 years. Throughout, our focus has been on illuminating the issues identified in their infancy, fostering greater understanding and informing public discussion.

This anthology contains only a small sample of the work we've done over the past 20 years. There is much more, all of which can be found at our website **www.ipc.on.ca**. I'm very proud of the breadth and depth of our work and encourage you to explore our website.

It's been a good 20 years for this Office. And much as I would like to imagine a future where a culture of privacy has become so engrained that a Commissioner is no longer necessary, I suspect that we still have some exciting days ahead of us to come!

Ann Cavoukian, Ph.D.
Information and Privacy Commissioner of Ontario

Table of Contents

Biometric Encryption:
A Positive-Sum Technology that Achieves Strong Authentication, Security AND Privacy

March 2007

Abstract

This paper discusses privacy-enhanced uses of biometrics, with a particular focus on the privacy and security advantages of Biometric Encryption (BE) over other uses of biometrics. The paper is intended to engage a broad audience to consider the merits of the Biometric Encryption approach to verifying identity, protecting privacy, and ensuring security. Our central message is that BE technology can help to overcome the prevailing "zero-sum" mentality, namely, that adding privacy to identification and information systems will necessarily weaken security and functionality. This paper explains how and why BE technology promises a "positive-sum," win-win scenario for all stakeholders involved.

Background / Context

Identification and authentication requirements are steadily increasing in both the online and offline worlds. There is a great need on the part of both public and private sector entities to "know" who they are dealing with. The current security model for the verification of identity, protection of information, and authorization to access premises or services is based on using a token, tied to and thereby representing an individual, to either authenticate identity or allow access to information, premises or services. This token may be a password or shared secret [something you know], an identity card (something you have), or a biometric (something you are). In all of these cases, the details of the token are held by a third party whose function is to authorize and at times allow the transaction to proceed if the details of an individual's token match those stored in a database. The biometric is increasingly viewed as the ultimate form of authentication or identification, supplying the third and final element of proof of identity. Accordingly, it is being rolled out in many security applications.

Privacy-related areas involving the protection of personal information, however, are not as strong – biometrics have not yet been able to fill this need. When an individual provides his or her personal information (financial or medical) to a second party, this party often stipulates that it will only use the personal information for the agreed-upon function, and will thereafter protect the information from access by unauthorized parties. The relationship between the individual who provides the information and the second party is largely based on a model of trust.

The trust model is becoming far less effective as current technological and geo-political situations evolve. The selling or sharing of personal information is now a lucrative business model practiced by many companies. Similarly, with increased threats of terrorism, governments and law enforcement agencies can now demand access to more and more personal information. With the growing powers of the Internet, extensive electronic dossiers may now be developed about an individual, without his or her knowledge or consent. Of even greater concern, perhaps, are the errors that can easily arise, which may then adversely affect that individual's life.

These dossiers may also include the details of token-based transactions such as biometrics, resulting in surprisingly complete dossiers about individuals and their transactional histories, again without their knowledge or consent. In turn, this precludes one's ability to ever correct any errors which may be contained in such databases, presenting an ever growing problem. In short, unauthorized access to one's personal information can result in a host of negative consequences ranging from identity theft and harassment to the perpetuation of mistakenly used personal information.

We acknowledge that government and law enforcement agencies require personal information to protect public safety and national security, while businesses require personal information to improve business practices and customer service. However, within these scenarios, the existing model of protecting privacy and safeguarding information invariably leads to a zero-sum game – protecting privacy often leads to less security and more costly business practices. This need not be the case.

Protecting public safety and a nation's security is a necessary and important function of a civilized society; developing more efficient business practices which are more cost effective and lead to better customer service are also highly desirable. Social and economic well-being are served by both of these functions.

However, liberty and freedom of choice are also essential to the functioning of prosperous and free societies. Technological advances in the collection and processing of information over the last few decades have positioned this resource as vital to the health, well-being and freedom of individuals. More specifically, abuses of personal information can cause untold harm, wasted resources, and generally lead to the detriment of society. For example, a society of individuals perpetually anxious about identity theft, misuses of their information, or unwarranted search and seizures cannot function at optimum levels.

It is our belief that the security model in current use must change from a zero-sum to a positive-sum paradigm where both the need for privacy / protection of personal information and the need for security can be satisfied. Accordingly, in this paper, we present what we believe to be the first step in the achievement of that goal through a new positive-sum model for both protecting information and providing security, based on "Biometric Encryption."

Growing Public Awareness and Interest

Biometrics are expected to add a new level of security to applications, as a person attempting access must prove who he or she really is by presenting a biometric to the system. Such systems may also have the convenience, from the user's perspective, of not requiring the user to remember a password.

There is evidence of growing public awareness and interest in the use of biometrics.

Border Security Control: Perhaps the most visible (and controversial) use of biometrics is taking place in the transportation sector. Identification requirements at airports and

border crossings may now involve the collection and processing of travellers' fingerprints, facial images, and iris patterns. Increasingly, machine readable travel documents such as passports, driver's licenses and other identity or travel cards may also contain biometric data or images. Frequent travelers who apply for and pass extensive background checks may use their biometrics for speedy passage through customs and immigration.

Crime and Fraud Prevention, Detection, and Forensics: The use of fingerprints by law enforcement has taken place for many years, but now that fingerprints can be digitized, stored, retrieved and matched instantaneously, many new uses have emerged, such as for populating watch lists and carrying out private sector background checks. In some parts of the United States, cashing a cheque can require a biometric imprint to be placed on the obverse side. Not a day goes by where the public is not apprised of some new "revolutionary" biometric technology that promises to solve crimes, catch villains and generally make the world a better place to live.

Attendance Recording: Employees and students are being required, in growing numbers, to present a biometric (such as a finger or hand) in order to "check in" to premises, much like a punchclock, or to claim some entitlement such as a luncheon meal or to check out a library book.

Payment Systems: We are seeing increasing uses of biometrics by the private sector for enhanced convenience services, such as "pay 'n' go" systems that allow enrolled customers to pay for groceries or gasoline using only their finger – at times, an enormous convenience.

Access Control: One of the most widespread uses of biometrics has been for physical and logical access to secure areas or resources (e.g. to a database of medical records, or accessing a laptop). In such circumstances, biometrics can enhance security by helping to ensure that access to sensitive resources is strictly restricted to authorized individuals.

A Biometrics Primer

"Biometrics" refers to automatic systems that use measurable, physical or physiological characteristics or behavioural traits to recognize the identity, or verify/authenticate the claimed identity of an individual. The examples of biometric characteristics that have been used for automated recognition include fingerprints, iris, face, hand or finger geometry, retina, voice, signature, and keystroke dynamics.

These systems are based on the following steps: a biometric sample is taken from an individual, for instance, a fingerprint or iris scan. This physical characteristic may be presented by an image. Often data are extracted from that sample. These extracted data constitute a *biometric template*. The biometric data, either the image or the template or both, are then stored on a storage medium. The medium could be a database or a distributed environment, such as smart cards. These preparatory phases together constitute the process of *enrolment*. The person whose data are thus stored is called the enrolee.

The actual purpose of the biometric system is only achieved at a later stage. If a person presents herself to the system, the system will ask her to submit her biometric characteristic(s). The system will then compare the image of the submitted sample (or the template extracted from it) with the biometric data of the enrolee. If the match succeeds, the person is then recognised and the system will "accept" her. If the match does not succeed, she is not recognized and she will be "rejected."

Traditional Biometrics: Privacy vs. Security – A Zero-Sum Game

We thought it might be useful to begin with a table that summarized the essential differences between the traditional zero-sum approach to biometrics vs. the positive-sum, Biometric Encryption approach. Such a comparison facilitates ease of reference and differentiates one from the other; this is also followed by the page number where a full discussion of the issue takes place.

Applicable law and regulation will vary, but biometric data, being derived from human bodies (and especially when used to identify or verify those bodies) is considered **personally identifiable information (PII)**. The collection, use and disclosure of biometric data — image or template — invokes rights on the part of an individual and obligations on the part of an organization.

Difficult ethical and operational questions surround the collection and use of video images used for facial recognition (which may be collected without the knowledge or consent of the individual), and of fingerprints and DNA samples, which may also reveal far more than identity.

As biometric uses and databases grow, so do concerns that the personal data collected will not be used in reasonable and accountable ways. Privacy concerns arise when biometric data are used for secondary purposes, invoking "function creep," data matching, aggregation, surveillance and profiling. Biometric data transmitted across networks and stored in various databases by others can also be stolen, copied, or otherwise misused in ways that can materially affect the individual involved.

A broad discussion of the various privacy implications of biometrics is available on the website of the Information and Privacy Commissioner of Ontario, **www.ipc.on.ca**[1].

Biometric Identification vs. Verification

Regardless of specific uses and deployment scenarios, most biometric systems will serve one of two foundational purposes: **identification** or **verification/authentication**.

Identification refers to the ability of a computer system to uniquely distinguish an individual from a larger set of individual biometric records on file (using only the biometric data). So, theoretically, a national biometric identification system could allow a citizen to prove who he or she is without recourse to any document — assuming the citizen was already registered in the system. The presented biometric data would

1 e.g. "Privacy and Biometrics," "Biometrics and Policing: Comments from a Privacy Perspective," and "Biometrics and Consumer Applications." All documents are freely available at **www.ipc.on.ca**.

	Traditional Biometrics: Privacy or Security A Zero-Sum Game	**Biometric Encryption: Privacy and Security – A Positive-Sum Game**
1	The biometric template stored is an identifier unique to the individual.	There is no conventional biometric template, therefore no unique biometric identifier may be tied to the individual. (pp. 18, 19)
2	Secondary uses of the template (unique identifier) can be used to log transactions if biometrics become widespread.	Without a unique identifier, transactions cannot be collected or tied to an individual. (pp. 19)
3	A compromised database of individual biometrics or their templates affects the privacy of all individuals.	No large databases of biometrics are created, only biometrically encrypted keys. Any compromise would have to take place one key at a time. (pp. 25)
4	Privacy and security not possible.	Privacy and security easily achieved. (pp. 19-22, 28-30)
5	Biometric cannot achieve a high level of challenge-response security.	Challenge-response security is an easily available option. (pp. 28-30)
6	Biometrics can only indirectly protect privacy of personal information in large private or public databases.	BE can enable the creation of a private and highly secure anonymous database structure for personal information in large private or public databases. (pp. 21, 22, 29-30)
7	*1:many* identification systems suffer from serious privacy concerns if the database is compromised.	*1:many* identification systems are both private and secure. (pp. 22)
8	Users' biometric images or templates cannot easily be replaced in the event of a breach, theft or account compromise.	Biometrically encrypted account identifiers can be revoked and a new identifier generated in the event of breach or database compromise. (pp. 19)
9	Biometric system is vulnerable to potential attacks.	BE is resilient to many known attacks. (pp. 20)
10	Data aggregation.	Data minimization. (pp. 19)

simply be compared with all other entries in the national database for a match, and upon a successful match the associated citizen's identity data would be released from the database. This is often referred to as a *"one-to-many"* match, and is used by police to identify criminals on watchlists, as well as by governments to identify qualified recipients for benefit-entitlement programs and registration systems such as voting, driver's license and other applications. So, for example, the facial images supplied in support of passport or driver's license applications could be routinely compared against large databases to ensure that multiple documents had not been issued to the same applicant (i.e., fraud detection).

Biometric **verification** or authentication involves a *"one-to-one"* search whereby a live biometric sample presented by a person is compared to a stored sample (on a smart card or contained in a database) previously given by that individual, and the match confirmed. The eligibility of the person for the service or benefit has already been previously established. The matching of the live biometric to the sample is all that is necessary to authenticate the individual as an eligible user. There need not be any search or matching to a central database, although a central database can still be used, provided that some other identification data is used. For example, an identity card's serial number could be used to "look up" an individual in a biometric database, and the live biometric sample could then be matched against the sample stored on record to verify the individual as the rightful bearer of the card. Even simpler, the person could just type in his username, so that his biometric template could be called up from the database for verification.

Identification templates are always stored in a database which is controlled by a custodian. *One-to-one* templates can be stored either in a database or in a distributed medium carried by a user (e.g. a passport, a smart card, or token). In the latter case, the user retains control over his biometric template.

Some current deployments require both identification and verification. For example, if a person applies for a passport/ID card, his biometric samples enter a *one-to-many* search first. This is done to check his background, i.e., to make sure that the person has not been listed in a criminal/ terrorist database before, usually under different identity. If the person is cleared, he is issued the passport/ID card to be used in a *one-to-one* system later on.

Somewhere between *"one-to-many"* identification and *"one-to-one"* authentication lies *"one-to-few"* biometric data uses, where "few" is of an order of 2–10,000. For example, a biometric lock may store the templates from all the members of a household or a firm. Some tokenless access control systems operate on this basis: the employee or user simply presents a biometric sample to the system, which then compares the sample against a small database of authorized users. If a match occurs, access is granted. The individual is both "identified" and "verified" as an authorized user — no other form of identification takes place.

Problems with using Biometrics for Identification Purposes

In the futuristic film *Minority Report* starring Tom Cruise, individuals are automatically and instantaneously identified via a millisecond remote scan of their irises. To escape detection, individuals must literally change their eyeballs. Thankfully, this scenario isn't likely to happen for some time because, for various reasons, biometric technologies are not well suited for large-scale *one-to-many* real-time identification purposes.

It is important to bear in mind that the collection of biometric samples and their processing into biometric templates for matching is subject to great variability. Simply put, biometrics are "fuzzy" – no two samples will be perfectly identical. Facial recognition technologies, for example, are notoriously prone to variability due to different lighting conditions, angle, subject movement, and so forth. This is the reason, for example, that we are asked not to smile in our passport photos. Similarly, numerous factors affect the ability to obtain reliable and consistent fingerprint samples. Among the various biometric types, irises seem to be the most accurate and consistent.

As a consequence, live biometric samples can be at some variance with stored reference samples, making comparison, matching and identification an inexact process. In other words, biometric systems do not have 100 per cent accuracy. When the biometric system cannot perform a proper match and (incorrectly) rejects a legitimate user, this is called a *false reject*, and the user must typically resubmit one or more biometric samples for further comparison by the system.

Biometric system designers can and do take measures to lower the *false rejection rate* (FRR) of their systems so this variability is smoothed out and the system can function properly. Apart from controlling the conditions under which fresh samples are taken, and improving the mathematical algorithms, one way to do this is to lower the threshold for matches to occur. However, the difficulty with this approach is that this often increases the *false acceptance rate* (FAR) of the system, that is, the system will incorrectly match a biometric to the wrong stored reference sample, resulting in misidentification. Usually there is a tradeoff between FRR and FAR, i.e., one error rate may only be reduced at the expense of the other (for example, some applications require lower FRR but can tolerate higher FAR, and vice versa).

The FRR/FAR numbers quoted by biometric vendors are often unreliable. The reader is advised to consult reputable independent sources of information, such as, for example, biometric competitions organized by the U.S. National Institute of Standard (NIST)[2], or International Fingerprint Verification Competitions (FVC2000/2002/2004)[3]. For most biometric systems, FRR ranges from 0.1% to 20%, meaning that a legitimate user will be rejected from one out of 1,000 times to one out of five times on average. FAR ranges from one in 100 (low security applications) to one in 10,000,000 (very high security applications).

Other challenges for a biometric system are speed (the system must make an accurate decision in real time), and security (the system must be resilient against attacks).

2 **http://www.frvt.org/; http://fpvte.nist.gov/; http://fingerprint.nist.gov/minex04/**

3 **http://bias.csr.unibo.it/fvc2004/**

So far, we have presented a straightforward technical discussion of the critical concepts of FAR and FRR. Now, we will consider the operational consequences and impacts of these rates for *one-to-many* identification purposes.

Assume, for example, a biometric identification system with a 0.01% FRR and 0.0001% FAR (an unlikely high accuracy, we acknowledge). That is, the system is able to consistently match a genuine biometric sample 9,999 times out of 10,000 attempts on average. As remarkably efficient as this system sounds, a single biometric sample, when compared against a database of 1,000,000 samples, will generate on average one false accept in addition to one exact match (if the user was actually enrolled in the database).

Now assume a database of 30,000,000 entries; each biometric sample would generate about 30 false accepts, each and every time! Clearly, this would be unacceptable for any real-time automatic identification system and would require significant human intervention in order to function.

Consequently, biometric system designers have resorted to other techniques to overcome the inherent technological problems of *one-to-many* identification. One way to significantly improve accuracy is to collect and compare *multiple* biometric samples. Multi-modal biometrics, for example, can involve collecting and using two (or more) fingerprints instead of one. If one fingerprint generates dozens or hundreds of false accepts, then the likelihood that two fingerprints will falsely match others in the database diminishes considerably. This is the primary reason behind emerging international requirements for including two separate biometrics (face and finger, for example), in machine-readable travel documents such as passports.

The privacy issue here, of course, involves the fact that more and more biometric samples of personal information need to be collected, transmitted, stored, and processed in order for the system to function properly. The FBI Integrated Automated Fingerprint Identification System (AFIS), containing hundreds of millions of records, for example, uses all 10 fingerprints for increased accuracy and speed. The US-VISIT program also plans to migrate from two fingerprints to 10 fingerprints and to develop the interoperability between US-VISIT and IAFIS[4].

Significant privacy (and operational) concerns arise with unrestricted collection and use of more and more biometric data for identification purposes. To begin with, the creation of large centralized databases, accessible over networks in real-time, presents significant operational and security concerns.

If networks fail or become unavailable, the entire identification system collapses. Recognizing this, system designers often build in high redundancy in parallel systems and mirrors (as well as failure and exception management processes) to ensure availability. However, this can have the effect of increasing the security risks and vulnerabilities of the biometric data.

4 **http://www.gao.gov/new.items/d07278.pdf**

Large centralized databases of biometric PII, hooked up to networks and made searchable in a distributed manner, represent significant targets for hackers and other malicious entities to exploit. It is also a regrettable reality that large centralized databases are also more prone to function creep (secondary uses) and insider abuse. There are also significant risks associated with transmitting biometric data over networks where they may be intercepted, copied, and actually tampered with, often without any detection.

Some large-scale biometric identification databases (such as the IAFIS, cited above) not only collect and file multiple biometric samples but, in an effort to preserve maximum compatibility with other fingerprint identification systems, store the full and complete *images* of the biometrics involved in addition to the templates! Proposed international standards for biometric-enabled machine-readable travel documents, for example, call for storage of the biometric *images* in the document rather than a structured reduction of the biometric into a unique template, in order to facilitate cross comparison and identification with other databases.

Storing, transmitting and using biometric *images* only exacerbates the privacy concerns with large-scale identification systems, since a very important privacy protection afforded by templates is removed, namely, the inability to *exactly* reconstruct the original biometric image from the template.

The image, conversely, can be converted into hundreds of templates for matching and identification (or other unknown or illegal) purposes such as creating personal profiles and, let us not forget, for committing identity theft. **At this point, the privacy implications explode.**

It should be evident that the loss or theft of one's biometric image opens the door to massive identity theft if the thief can use the biometric for his or her own purposes. For example, the ability to create low-cost duplicate fake fingerprints from "gummy bears," which are capable of fooling nine out of 10 biometric systems, has been well-documented.[5] Others have even documented how easy it is to fool a biometric system by presenting it with a photograph! Of course, the biometric industry has come up with countermeasures, such as "liveness detection" of a finger, or capturing 3D face images, but so will the attackers in this perpetual game. Moreover, in the digital realm, there may be no need to even present a "fake finger" if all that is required is the digital equivalent, which can be supplied to the network instead.

Even worse, in all of these identification scenarios, the biometric effectively serves as an index or key to the database involved, much like login usernames serve to identify registered users of a computer network.

But, because people usually only have two thumbs, two eyes, and one head, it is nearly impossible to change these if and when the related biometric data become compromised. In this sense biometrics operate like shared secrets or passwords – learn the

5 T. Matsumoto, H. Matsumoto, K. Yamada, S. Hoshino, "Impact of Artificial Gummy Fingers on Fingerprint Systems," Proceedings of SPIE Vol. #4677, Optical Security and Counterfeit Deterrence Techniques IV, 2002.

secret and you're in! But there are some very important difference between biometrics and passwords: you cannot change them and have no choice but to keep them for life. Lose control of your lifetime password and you will have some explaining to do! This, regardless of the fact that security experts roundly condemn using unchangeable passwords as shared secrets (e.g. birthdates and SINs).

Views of the Privacy Community

The global privacy and data protection community have consistently argued *against* the use of biometrics for most *one-to-many* identification purposes, and *against* the creation of large, centralized or interoperable databases of biometric data:

- Resolution of International Data Protection Authorities;[6]
- Opinions of the European EDPS and Article 29 Working Party;[7] and
- Publications and testimony of Ontario Information and Privacy Commissioner.

The global privacy community has insisted on building privacy-enhancing technologies (PETs) directly into biometrics systems wherever possible, to ensure that they reflect the requirements of Fair Information Principles and Practices and applicable privacy laws regarding the collection, use and disclosure of PII. Privacy, consumer, and civil rights advocates around the world have strongly favoured limiting the use of biometrics for verification/authentication purposes, especially in distributed environments (where the biometric sample is retained by the user on a token, say, a smart card[8]).

Deployment Experience to Date

The reality is that the highly-lauded use of privacy-enhanced *one-to-one* biometric authentication technologies has simply not been widespread. Perhaps the best-known example has been its deployment in laptop computers, where users must match their biometric (fingerprint) in order to gain access to the laptop.

Public sector government bodies, on the other hand, have tended to insist on building large-scale interoperable biometric databases. The reasons for this preference are complex and worthy of exploration in a separate research paper. Briefly, however, some possible explanations are as follows:

- The claim of overriding public interests or (secondary) purposes that override individual privacy interests. It is here that the "zero-sum" game mentality prevails, i.e., more individual privacy equals less public security, and vice-versa;

6 International Data Protection Commissioners, "Resolution on the use of biometrics in passports, identity cards and travel documents," Montreux (September 2005) available at: **www.edps.europa.eu/legislation/05-09-16_resolution_biometrics_EN.pdf**

7 See Appendix 1 for documents and sources

8 In the "real" world the template or biometric image would be stored in a database as a backup in case the user lost his or her card. Otherwise, users would have to re-enroll every time they misplaced or lost their token. However, these databases would be limited and not networked, and encrypted.

- Unwillingness of system designers and operators to relinquish control over biometrics to individual users. Here, too, adding privacy is often viewed as compromising system functionality, control, and effectiveness;
- Requirements to carry out more and more background checks (e.g. against criminal records, terrorist watch lists, etc.) or to prevent multiple identity registrations and benefits fraud (welfare, medicare, driver licenses, immigration applications, etc.);
- Need to retain evidence and to make a criminal case when necessary (only biometric images verified by a human expert are accepted by courts, not just templates);
- Backup needs and escrow requirements – copies of biometric data need to be retained on file and made available to system operators and other authorities "just in case" the system fails;
- Unavailability of suitable, reliable, and cost efficient privacy-enhanced biometric technologies and systems;
- Unreliable biometric enrolment/verification procedures and practices, which undermine ALL biometric systems if attackers can fraudulently impersonate others;
- Strong pressure from technology vendors and/or advice from independent consultants and integrators who may lack incentives to pursue privacy-enhanced biometric system options;
- The simplistic conflation of privacy and security, i.e., the misguided (and erroneous) belief that all biometric privacy interests can be satisfied by building system controls that seek to ensure confidentiality and integrity of the biometric data. This is a very common problem among security professionals, who tend to undervalue privacy as a separate and unique set of design principles; and
- Weak public demand and guidance from the privacy and data protection communities.

The reader will note that most of these explanations are predicated on zero-sum game thinking; i.e., more individual privacy and user control equals less of virtually everything else! Taken from this view, building true biometric privacy into an information system is invariably seen as a cost, rarely as an enhancement.

A more common deployment scenario is to carry out *one-to-one* biometric authentication *against a single stored sample in a database*. For example, a biometric-enabled identity card may have a serial number that acts as an index or lookup key to the database, calling up the biometric "password" for *one-to-one* comparison and authentication against a live sample.

Security Vulnerabilities of a Biometric System

Biometric systems, especially *one-to-one*, may become vulnerable to potential attacks.[9]

Some of those security vulnerabilities include the following:

- **Spoofing.** It has been demonstrated that a biometric system sometimes can be fooled by applying fake fingerprints, face or iris image, etc.
- **Replay attacks,** e.g. circumventing the sensor by injecting a recorded image in the system input – much easier than attacking the sensor.
- **Substitution attack:** The biometric template must be stored to allow user verification. If an attacker gets an access to the storage, either local or remote, he can overwrite the legitimate user's template with his/her own – in essence, stealing their identity.
- **Tampering:** Feature sets on verification or in the templates can be modified in order to obtain a high verification score, no matter which image is presented to the system.
- **Masquerade attack.** It was demonstrated[10] that a digital "artefact" image can be created from a fingerprint template, so that this artefact, if submitted to the system, will produce a match. The artefact may not even resemble the original image. This attack poses a real threat to the remote authentication systems (e.g. via the Web), since an attacker does not even have to bother to acquire a genuine biometric sample. All he needs is just to gain an access to the templates stored on a remote server (this perfectly fits a description of a typical hacker operating from a rat hole).
- **Trojan horse attacks:** Some parts of the system, e.g. a matcher, can be replaced by a Trojan horse program that always outputs high verification scores.
- **Overriding Yes/No response.** An inherent flaw of existing biometric systems is due to the fact that the output of the system is always a binary Yes/No (i.e., match/no match) response. In other words, there is a fundamental disconnect between the biometric and applications, which makes the system open to potential attacks. For example, if an attacker were able to interject a false Yes response at a proper point of the communication between the biometrics and the application, he could pose as a legitimate user to any of the applications, thus bypassing the biometric part.
- Insufficient accuracy of many commercial biometric systems, both in terms of FRR and FAR. High FRR causes inconvenience for legitimate users and prompts the system administrator to lower a verification threshold. This inevitably gives rise to FAR, which, in turn, lowers the security level of the system.

9 N. K. Ratha, J. H. Connell, R. M. Bolle. Enhancing security and privacy in biometrics-based authentication systems. IBM Systems Journal, vol. 40, NO 3, p.p. 614 – 634, 2001.

10 C.J. Hill, "Risk of masquerade arising from the storage of biometrics," B.S. Thesis, Australian national University, 2001 (supervisor – Dr. Roger Clarke). **http://chris.fornax.net/biometrics.html**

The privacy and security issues of a biometric system outlined in this section are illustrated in Fig. 1.

An enrolment part of any conventional biometric system consists of at least three blocks: a biometric sensor which acquires an image, a feature extractor that creates a biometric template, and a storage for the templates, or images, or both. The storage can be either a database or a distributed medium.

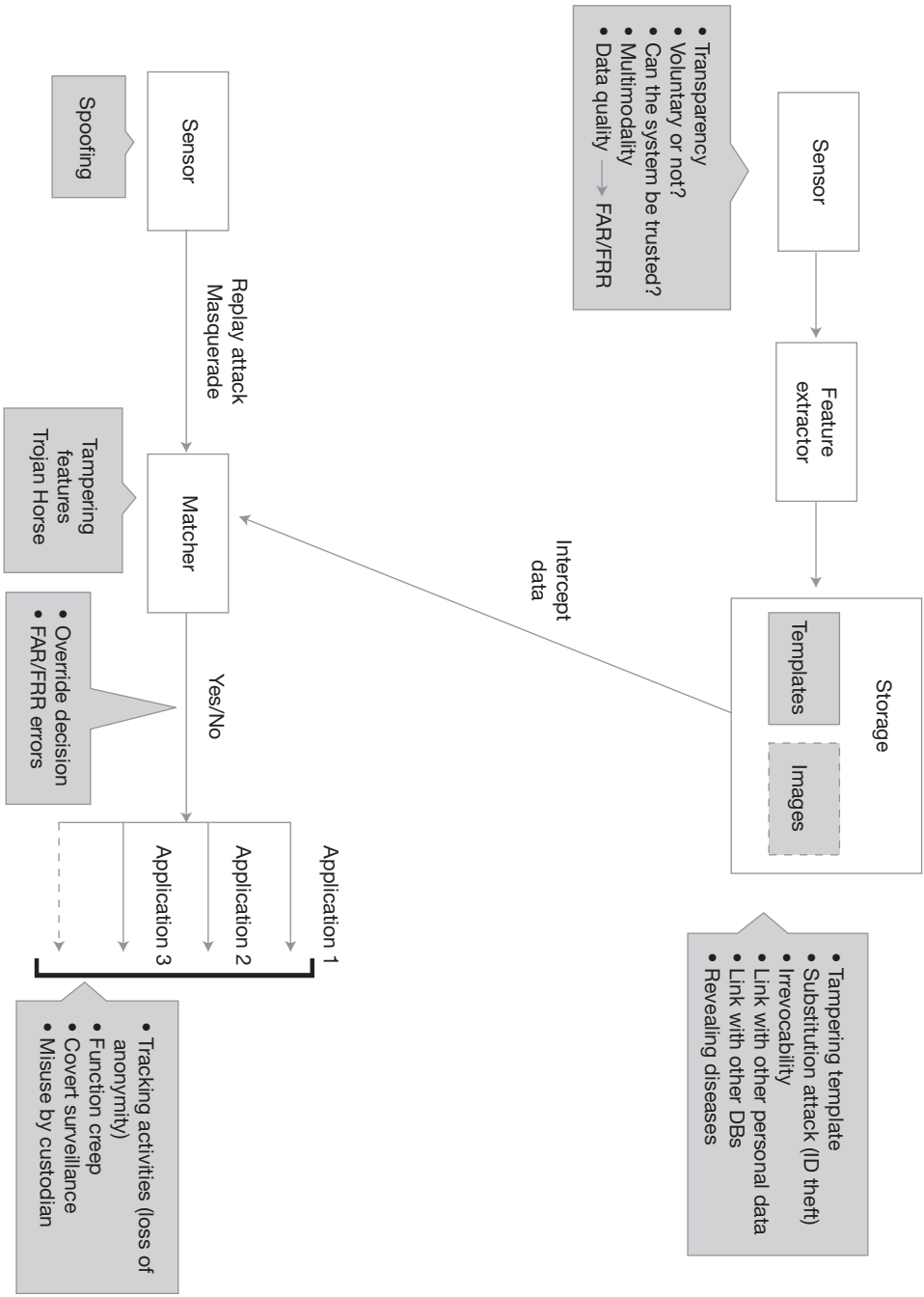
A verification or identification part contains (at a minimum) a sensor to acquire a new image sample, and a matcher, which compares the image with the previously enrolled template(s) received from the storage. The output of the matcher is a Yes/No (i.e., match/no match) response that may go to the variety of applications.

A user of the system faces several privacy issues immediately at enrolment:

- Transparency, i.e., if the purpose of the system is clear to the user;
- If the enrolment is voluntary, and what are the consequences of not getting enrolled (for a variety of reasons);
- If the system can be trusted, i.e., if the personal data are adequately protected;
- Quality of biometric data: poor quality may lead to higher FRR and FAR. While FAR increases security risks for the system, a false rejection often causes some follow-up procedures which can be privacy-invasive to the individual.

Other privacy/security issues were explained in the foregoing sections.

Figure 1: Privacy and security issues involving a biometric system



Biometric Encryption

Biometrics and Cryptography

Conventional cryptography uses encryption keys, which are just bit strings long enough, usually 128 bit or more. These keys, either "symmetric," "public," or "private," are an essential part of any cryptosystem, for example, Public Key Infrastructure (PKI). A person cannot memorize such a long random key, so that the key is generated, after several steps, from a password or a PIN that can be memorized. The password management is the weakest point of any cryptosystem, as the password can be guessed, found with a brute force search, or stolen by an attacker.

On the other hand, biometrics provide a person with unique characteristics which are always there. Can they be used as a cryptographic key? Unfortunately, the answer is negative: biometric images or templates are variable by nature, i.e., each new biometric sample is always different. Needless to remind that conventional cryptography does not tolerate a single bit error.

As noted in the previous chapter, a biometric system always produces a Yes/No response, which is essentially one bit of information. Therefore, an obvious role of biometrics in the conventional cryptosystem is just password management, as mentioned by Bruce Schneier.[11] Upon receiving Yes response, the system unlocks a password or a key. The key must be stored in a secure location (so called "trusted" device). This scheme is still prone to the security vulnerabilities noted in Fig. 1, since the biometric system and the application are connected via one bit only.

Biometric templates or images stored in a database can be encrypted by conventional cryptographic means. This would improve the level of system security, since an attacker must gain the access to the encryption keys first. However, most privacy issues associated with a large database remain, since the keys and, therefore, the biometric data, are controlled by a custodian.[12]

A comprehensive review of the issues involving biometrics and cryptography can be found elsewhere.[13]

What is Biometric Encryption?

Because of its variability, the biometric image or template itself cannot serve as a cryptographic key. However, the amount of information contained in a biometric image is quite large: for example, a typical image of 300x400 pixel size, encoded with eight bits

11 B. Schneier, "The Uses and Abuses of Biometrics," Comm. ACM, vol. 42, no. 8, p. 136, Aug. 1999.

12 There has been recent activity of International Organization for Standardization in order to support the confidentiality and integrity of the biometric template by using cryptographic means (ISO/IEC WD 24745, "Biometric Template Protection"): **www.nia.din.de/sixcms/media.php/1377/SC27N4997rev1_SD7_Catalog_Proj&Stand_May2006.htm ?backend_call=true#24745; www.incits.org/tc_home/CS1/2007docs/cs1070006.pdf**

13 "Future of Identity in the Information Society" (FIDIS) report, "D3.2: A study on PKI and biometrics," 2005. **www.fidis. net/fileadmin/fidis/deliverables/fidis-wp3-del3.2.study_on_PKI_and_biometrics.pdf**

per pixel has 300x400x8 = 960,000 bits of information. Of course, this information is highly redundant. One can ask a question: Is it possible to consistently extract a relatively small number of bits, say 128, out of these 960,000 bits? Or, is it possible to bind a 128 bit key to the biometric information, so that the key could be consistently regenerated? While the answer to the first question is problematic, the second question has given rise to the new area of research, called Biometric Encryption (BE).[14]

Biometric Encryption is a process that securely binds a PIN or a cryptographic key to a biometric, so that neither the key nor the biometric can be retrieved from the stored template. The key is re-created only if the correct live biometric sample is presented on verification.

> **"In Biometric Encryption, you can use the biometric to encrypt a PIN, a password, or an alphanumeric string, for numerous applications – to gain access to computers, bank machines, to enter buildings, etc. The PINs can be 100s of digits in length; the length doesn't matter because you don't need to remember it. And most importantly, all one has to store in a database is the biometrically encrypted PIN or password, not the biometric template."**
>
> Dr. George Tomko, OECD Report on Biometric-Based Technologies (2004)[15]

The digital key (password, PIN, etc.) is randomly generated on enrolment, so that the user (or anybody else) does not even know it. The key itself is completely independent of biometrics and, therefore, can always be changed or updated. After a biometric sample is acquired, the BE algorithm securely and consistently binds the key to the biometric to create a protected BE template, also called "private template." In essence, the key *is encrypted* with the biometric. The BE template provides excellent privacy protection and can be stored either in a database or locally (smart card, token, laptop, cell phone, etc.). At the end of the enrolment, both the key and the biometric are discarded.

On verification, the user presents her fresh biometric sample, which, when applied to the legitimate BE template, will let the BE algorithm retrieve the same key/password. In other words, the biometric serves as a *decryption key*. At the end of verification, the biometric sample is discarded once again. The BE algorithm is designed to account for acceptable variations in the input biometric. On the other hand, an attacker, whose biometric sample is different enough, will not be able to retrieve the password. This encryption/decryption scheme is *fuzzy*, as the biometric sample is different each time, unlike an encryption key in conventional cryptography. Of course, it is a big technological challenge to make the system work.

14 Other terms used for this technology: biometric cryptosystem, private template, fuzzy commitment scheme, fuzzy vault, fuzzy extractor, secure sketch, biometric locking, biometric key binding, biometric key generation, virtual PIN, biometrically hardened passwords, biometric signature, bioHashing. We use the term "Biometric Encryption" in a broad sense.

15 OECD *Report on Biometric-Based Technologies* (June 2004). Directorate for Science, Technology and Industry, Committee for Information, Computer and Communications Policy, DSTI/ICCP/REG(2003)2/FINAL, p. 64

After the digital key, password, PIN, etc., is retrieved, it can be used as the basis for any physical or logical application. The most obvious way lies in the conventional cryptosystem, such as a PKI, where the password will generate a pair of Public and Private keys.

Thus, Biometric Encryption is an effective, secure, and privacy friendly tool for biometric password management, since the biometric and the password are bound on a fundamental level.

Advantages of Biometric Encryption (over other Biometric Systems)

Biometric Encryption technologies have enormous potential to enhance privacy and security. Some of the key benefits and advantages of this technology include:

1 NO retention of the biometric image or template

From a privacy perspective, the best practice is not to collect any personally identifiable information (PII) at all in the first place, to the fullest extent possible. This is referred to as "data minimization" – minimizing the amount of personal data collected and retained, thus eliminating the possibility of subsequent abuse.

Most privacy and security concerns derive from storage and misuse of the biometric data.

A common concern is that "if you build it (the database), they will come (for the data)." The topline privacy and security concerns include fears of potential data matching, surveillance, profiling, interception, data security breaches, and identity theft by others. Misuse and mismanagement of biometric data by others invokes "negative externalities" and costs that fall primarily upon individuals rather than the collecting organization, but also at stake is the accountability and credibility of the collecting organization, and with them, the viability of the entire program.

Biometric Encryption directly addresses these risks, threats and concerns.

Users retain complete (local) control and use of their own biometrics.

Local control enhances confidence and trust in the system, which ultimately promotes greater enrolment and use.

2 Multiple / cancellable / revocable identifiers

Biometric Encryption allows individuals to use a single biometric for multiple accounts and purposes without fear that these separate identifiers or uses will be linked together by a single biometric image or template.

Thus, if a single account identifier becomes compromised, there is far less risk that all the other accounts will also be compromised.

Even better, Biometric Encryption technologies make possible the ability to change or recompute account identifiers. That is, identifiers may be revoked or cancelled, and substituted for newly generated ones calculated from the same biometric!

Traditional biometric systems simply cannot do this.

3 Improved authentication security: stronger binding of user biometric and identifier

Account identifiers are bound with the biometric and recomputed directly from it on verification.

This results in much stronger account identifiers (passwords):

- longer, more complex identifiers;
- no need for user memorization; and
- less susceptible to security attacks.

Many security vulnerabilities of a biometric system listed in Fig. 1 are addressed:

No substitution attack: An attacker cannot create his own template since he, or anybody else, does not know the digital key and other transitory data that had been used to create the legitimate template;

No tampering: Since the extracted features are not stored, the attacker has no way to modify them;

No masquerade attack: Again, the system does not store the biometric template, so that the attacker cannot create a digital artefact to submit to the system. Biometric Encryption provides an effective protection for remote authentication systems;

No Trojan horse attacks: BE algorithm does not use any score, either final or intermediate, to make a decision, it just retrieves (or does not retrieve) a key. Therefore, the attacker has no means to fool the system by outputting a high score;

No overriding Yes/No response: The output of BE algorithm is a 128-bit (or longer) digital key, as opposed to the binary Yes/No response. The attacker cannot obtain the key from a private template.

The security of Biometric Encryption technology can be augmented by the use of tokens (e.g. smart cards, PDA) and additional PINs, if needed.

4 Improved security of personal data and communications

As an added bonus, users can take advantage of the convenience and ease of Biometric Encryption technologies to encrypt their own personal or sensitive data. See Case Study #1 for an example.

Since the key is one's own biometric, used locally, this technology could place a powerful tool directly in the hands of individuals.

Biometric Encryption could be viewed as encryption for the masses, made easy!

5 Greater public confidence, acceptance, and use; greater compliance with privacy laws

Public confidence and trust are necessary ingredients for the success of any biometric system deployment. One major data breach or horror story involving a large centralized database of biometric templates could set back the entire industry for years.

Data governance policies and procedures can only go so far to foster public trust. However, if privacy, security and trust can be built directly into the biometric system, then the public and data protection authorities are far more likely to accept the privacy claims being made.

Putting biometric data firmly under the exclusive control of the individual, in a way that benefits that individual and minimizes risk of surveillance and identity theft, will go a long way towards satisfying the requirements of privacy and data protection laws, and will promote broader acceptance and use of biometrics.

6 Suitable for large-scale applications

Biometric Encryption technologies speak directly to the clear preference and recommendations of the privacy and data protection authorities for using biometrics to authenticate or verify identity, rather than for identification purposes alone.

Therefore, we prefer seeing biometrics used to positively link the bearer to a card or token, and to avoid creating systems that rely upon centralized storage and remote access/lookup of biometric data.

A prevailing reason for this view is that it is not known if biometric technology is sufficiently accurate and reliable to permit real time identification in large *n* samples, where *n* is of an order of several million or higher. Despite these views, many large-scale *one-to-many* public biometric projects are being proposed and are well underway.

Often the biometric data in these systems are actually used for authentication purposes and not identification, but the lines between these two concepts can be blurred when multiple data items are collected and transmitted to a database for comparison. What becomes the identifier and what becomes the authenticator is somewhat arbitrary.

From a privacy point of view, transmitting biometric image or template data to a central database to be authenticated is risky enough without compounding the risks by sending more and more personal identifiers with it. “Multimodal” biometric solutions depend on collecting and comparing more than one biometric. It should be noted that the main reason for using “multimodal” solutions, besides providing a fallback for problem users, is insufficient accuracy/speed/security of existing biometrics. So the technical “solution” to using biometrics for authentication seems to be to collect more and more biometric and other personal data.

In 2006, the European Data Protection Supervisor (EDPS) Peter Hustinx warned, in a formal opinion, of the privacy dangers of using biometric images or templates as an index or key to interoperable databases.[16]

Fortunately, Biometric Encryption technologies make possible database applications (see Case Study #3 as an example), minimizing the risks of traditional biometric systems (although we still prefer *one-to-one* applications with local template storage). It is possible to create secure and local biometric-enabled bindings of users to some other token identifiers without the need to reveal the actual biometric image or data.

It is further possible to create a so-called "anonymous database," where a link between an anonymous identifier and encrypted (by conventional cryptographic means) user's record is controlled by a Biometric Encryption process. This is very useful for a database containing sensitive information, such as medical records (see Case Study #2 for more details).

Another promising application of BE is a privacy-protected *one-to-many* database for "double dipping" prevention. The database is multimodal: it contains conventional but anonymous templates for one biometric, e.g. fingerprints, and private templates, e.g. for iris, that control a link with the user's encrypted records. A user's record would only be decrypted and displayed if there was a positive match on both conventional and private templates. Otherwise, all the information is inaccessible even to the system administrator.

With Biometric Encryption, users would be empowered by the ability to securely prove who they are to anyone, for any purpose, using their own biometrics, but without having to disclose the biometric data itself!

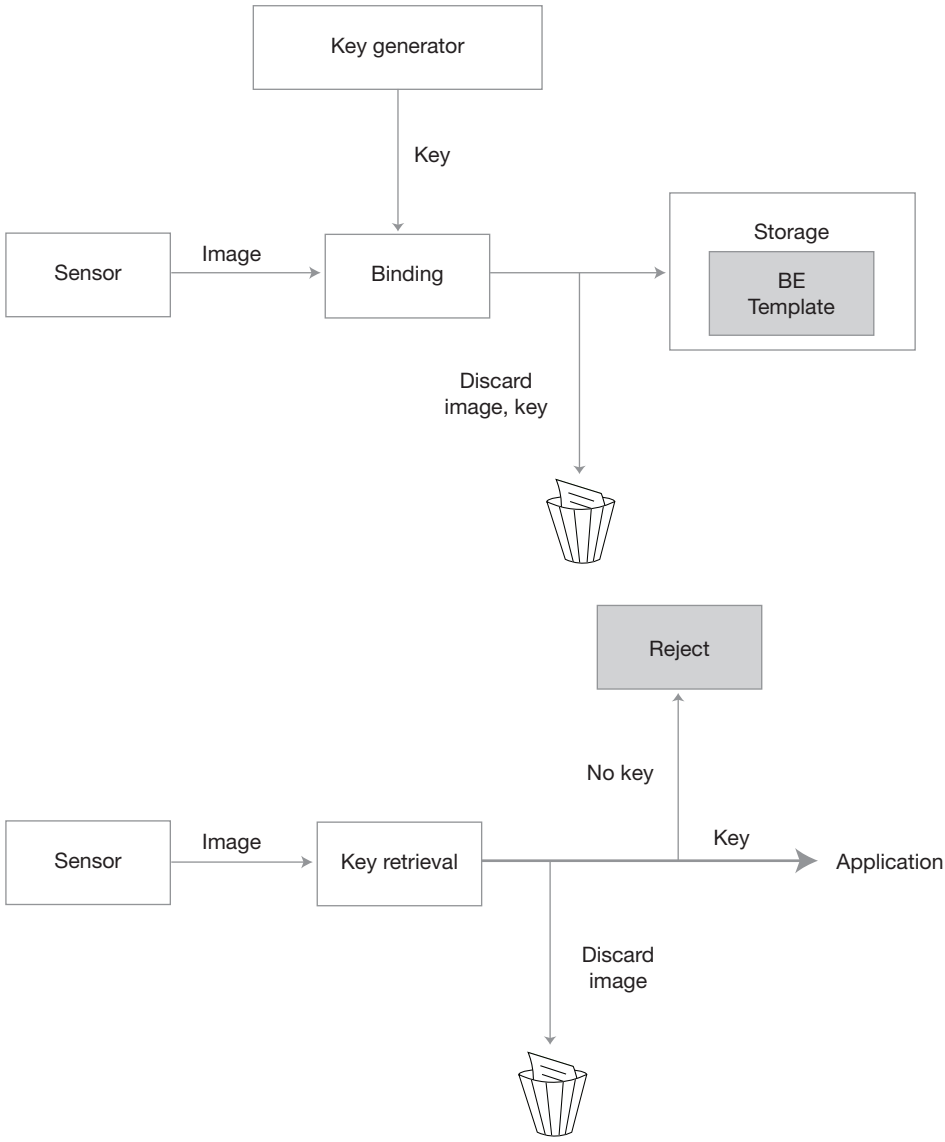
A high level diagram of a Biometric Encryption process is shown in Figure 2 (next page).

An enrolment part of a Biometric Encryption system consists of at least four blocks: a biometric sensor, a key generator that normally outputs a random key, a binding algorithm that creates a BE (private) template, and a storage for the BE template. Neither the key nor the image can be recovered from the BE template. The key, the image, and some transitory data are discarded at the end of the enrolment process.

A verification part contains at least a sensor to acquire a new image sample, and a key retrieval algorithm, which applies the image to the previously enrolled BE template received from the storage. The algorithm either retrieves the key, if the image on verification is close enough to the one enrolled, or fails to do so, in which case the user is rejected. The key enters an application, such as a PKI. Each application has its unique key. The biometric image is discarded at the end of the verification process.

16 See Appendix 1 for references and URLs

Figure 2: High level diagram of a Biometric Encryption process



Current State of Biometric Encryption

The original concept of Biometric Encryption for fingerprints was pioneered in 1994 by Dr. George Tomko, founder of Mytec Technologies (Toronto, Canada). Since then, many research groups have taken part in the development of BE and related technologies. There are about 50 articles and patents published to date, most of which appeared since 2002.The list of publications, with a brief review, is presented in Appendix 2.

Besides Biometric Encryption (BE), other terms have been used for this technology, such as: biometric cryptosystem, private template, fuzzy commitment scheme, fuzzy vault, fuzzy extractor, secure sketch, biometric locking, biometric key binding, biometric key generation, virtual PIN, biometrically hardened passwords, biometric signature, and bioHashing.

BE and related technologies have drawn attention from major academic research centres specializing in biometrics, such as Michigan State University, West Virginia University, Carnegie Mellon University, University of Cambridge (U.K.), and University of Bologna (Italy). Among current industry leaders, those worth noting include IBM T.J. Watson Research Center, RSA Laboratories, Lucent Technologies, Sandia National Laboratories, and Philips Research.

Virtually all types of biometrics have been tested to bind (or to generate) a digital key: fingerprints, iris, face, key stroke dynamics, voice, handwritten signatures, palmprints, acoustic ear recognition. The most promising results have been achieved with an iris: FRR = 0.47%, FAR = 0 (or at least less than one in 200,000) to generate a 140-bit key. These error rates are only marginally larger than for a conventional iris-based biometric system with the same input images[17]. The use of fingerprints is also feasible in terms of accuracy for BE, with FRR greater than 10% at present. Unlike an iris, there is a noticeable degradation in accuracy from a conventional fingerprint system. This is understandable since fingerprints are more prone to distortions and other factors that degrade accuracy. It is more difficult to compensate those factors in the case of Biometric Encryption, since BE works in a "blind" mode (the enrolled fingerprint or its minutiae template are not seen). There are several ways to overcome this problem, for example, by using a free air (i.e., contactless) fingerprint sensor, or by using more than one finger from the same person, or by combining several biometrics.[18]

Face recognition, which is usually considered third (after irises and fingerprints) in terms of accuracy in conventional biometrics, has shown a significant improvement of performance over the last few years. This allowed Philips Research to create a working BE system using a face biometric. The published results range from FRR = 3.5% for a face database with low to medium variability of images to FRR = 35% for a database with

17 The iris images were acquired in close to ideal conditions of a laboratory environment. In real life systems, some degradation of performance is expected, which is always the case with biometrics.

18 Note that even a 10% – 20% false rejection rate still may be acceptable for some applications with relatively low traffic and cooperative users: it simply means that a person would be rejected each fifth or tenth time on average and asked by the system to place the finger on the reader again.

high variability; FAR = 0 (or at least less than 1 in 100,000) in both cases. The key size used is 58 bits, which may be sufficient as a password replacement. According to communication from Dr. Michiel van der Veen of Philips Research, their technology, called privID™, is now operational and ready for deployment; in particular, it will be a part of a EU 3D Face project (WP2.5)[19]. To the best of our knowledge, the Philips system will be the first real life application of BE technology.

It is not clear if other biometrics have enough entropy (i.e., the amount of non-redundant information) in order to bind a sufficiently long key (e.g. 128 bit). This is an area of future research.

Some works published since 2002 provide a general theoretical foundation for BE technologies from a cryptographic point of view. They prove that the system can be made secure against "brute force" search attacks. In other words, an attacker checks at random all possible combinations in order to retrieve a key (or a biometric). Like conventional cryptography, it is assumed that the attacker is fully familiar with the algorithm, and may have a template in hand, but does not have a proper biometric to unlock the secret (i.e., the key bound to the biometric).

However, the attacker may try more sophisticated attacks exploiting inherent weaknesses (if any) of the BE system and biometrics in general. This area of research has been largely overlooked. If such an attack is successful, the effective security of the system would be reduced from 128 bits to, perhaps, 69, 44, or even lower number of bits. "This may seem an alarmingly small number to the crypto purist" (Hao, Anderson, and Daugman, 2005). On the other hand, BE is not just another cryptographic algorithm; it is rather a key/password management scheme. Key management has always been the weakest part of any cryptosystem, as it relies on passwords that may be forgotten, stolen, guessed, shared, etc. Biometric Encryption binds the key/password with the biometric and, thus, makes the system more secure. By comparison, a conventional biometric has only 1-bit security – a Yes/No response!

It is interesting to note that code-breaking becomes reduced to a security problem, not a privacy issue with BE, e.g. with an encrypted database of templates, breaking the encryption key exposes all the templates, and one has both a security and a privacy issue. Breaking a biometrically encrypted key, however, only exposes that key, but not necessarily the biometric, let alone the entire database, making it a far more secure system.

With the notable exception of Philips privID™, to the best of our knowledge, there is no other commercially available BE system being used to date. The reason for this lies in both the technological challenges and existing market conditions. Not only the general public, but most hi-tech developers are unaware of this emerging technology. Consequently, resources and funding in this area have, to date, been quite poor. We believe that the technological challenges have largely been overcome using an iris or face,

19 **www.3Dface.org**

and partially for fingerprints, bringing BE technology very close to the prototype development stage, and could soon be ready for testing in pilot projects.

Related Technologies

1. Storing a key in a trusted system

There have been some products[20] that store a cryptographic key or a PIN in a so-called trusted system (e.g. a computer or a Digital Signal Processor (DSP)). The key is released upon successful biometric verification and then enters a conventional cryptosystem, e.g. Public Key Infrastructure (PKI). The biometric template (or image) is also stored somewhere, often in encrypted (by conventional means) form.

If properly implemented, such systems may offer some security benefits. However, most problems outlined in the foregoing sections remain. For example, a binary Yes/No response is still required to release the key – this part of the algorithm is just hidden better. Most privacy issues associated with the template storage are also there.

Note that these systems often use the same terminology and/or claim the same benefits as BE, while in fact they do not provide a true binding between a key and a biometric.

2. Cancellable biometrics

A new area of research, closely related to BE, is called cancellable biometrics. It has been developed by IBM T.J. Watson Research Center, and by some academic groups. In this privacy-protecting technology, a distortion transform (preferably, irreversible) is applied to a biometric template. Only those distorted templates are stored, and they are matched also in the distorted form. If a distorted template is compromised, it can be "cancelled" by choosing just another distortion transform (i.e., the biometric is not lost). The transforms are application dependent, meaning that the templates cannot be reused by another applications (function creep is prevented).

Cancellable biometrics shares some other similarities with BE, for example, a technique called bioHashing can be used for both technologies. Unlike BE, a key is not generated or released in cancellable biometrics, so that the system still produces a binary Yes/No response and is more vulnerable to attacks. The distortion transform should be truly irreversible (i.e., one way only) and kept secret. Otherwise, an attacker can either reconstruct the original biometric or create his own impostor template for a substitution attack, or even create an "artefact" image for a masquerade attack. Since the key is not generated, the variety of potential applications is narrower than for BE; for example, an anonymous database cannot be created. On the other hand, BE possesses all the functionality of cancellable biometrics, and, therefore, is a *method* for cancellable biometrics. Both technologies face similar accuracy/security challenges.

20 See, for example: **www.ceelox.com; www.sequiam.com; www.lacie.com/products/product.htm?id=10166; and www. axistech.com/Biomeric_Time_attandance_Axis_Technology_Encryption.asp**

3. Fuzzy Identity Based Encryption

Another related technology, called Fuzzy Identity Based Encryption (FIBE), was proposed by A. Sahai and B. Waters in 2005. This technology also combines biometrics and cryptography on a fundamental level. Unlike BE, the user's biometric is made somewhat public. In an example provided by D. Nali, C. Adams and A. Miri (see also a webcast presentation by B. Waters)[21], a user (*A*) could go to a Driver Licensing Agency (*D*), and identify herself via an iris scan, under the ongoing surveillance of a trained agent. *D* could then use this scan to encrypt *A*'s information (e.g. an annual driver's license), when this information needs to be securely sent to *A* (e.g. via the Web). In order to obtain her biometric *private keys*, *A* would have to go in person to a trusted third party (e.g. a state agency) which would deliver keys via the same authenticating procedure as that used by *D. A* could then decrypt the message addressed to her using FIBE. She does not need a biometric reading at that point. In other words, *A* leaves her biometrics in at least two places, *D* and the trusted third party (often called Trusted Authority (TA)).

This scheme prevents impersonation of A by surreptitiously capturing her biometric sample, such as an iris photograph or latent fingerprints. "FIBE allows biometric measurements to be public" (Nali, Adams and Miri) and, therefore, those surreptitious samples would become useless. While interesting from a scientific point of view, this technology is not privacy protecting, at least in the sense adopted by the privacy community (biometric data are considered personal information). There are also problems in handling a false rejection: user *A* may not have a chance to present another biometric sample if the false rejection occurs during decryption.

Scientific, Technological, and Privacy-Related Merits

Encryption with a fuzzy key (such as a biometric) was only recently introduced in conventional cryptography. Beyond such trivial things like accepting a few spelling errors in a password, or letting Alice partially share a list of her favourite movies with Bob, Biometric Encryption technologies are by far the most important application of those theoretical works. Market demand for such a technology would provide a great incentive to this promising area of modern mathematics and cryptography.

BE results in tougher requirements for distortion tolerance, discrimination, and the security of a biometric system. Solving these problems would be a significant scientific breakthrough both in the area of biometrics and cryptography. This would accelerate research and development of better biometric sensors and other hardware, as well as new, more accurate algorithms and software. No doubt this would bring technological benefits for the entire biometrics.

BE overcomes many security vulnerabilities of a biometric system, especially in a distributed environment. This could facilitate deployment of biometric systems on portable and handheld devices (laptops, cellphones, PDAs, etc.).

21 **http://www.researchchannel.org/prog/displayevent.aspx?rID=3913**

It would not be an overstatement to say that biometrics is perceived, in general, as a privacy-invasive technology. As we have shown, this perception is not baseless. Biometric Encryption, on the other hand, is a *privacy-enhancing technology*. It allows a user to retain full control over her biometric and, at the same time, to stay anonymous in many applications, i.e., to be represented only by a randomly generated (and cancellable) identifier linked to her biometric. No other personal data, e.g. address, telephone, date of birth, have to be revealed.

BE can render databases privacy-protected, as they will comprise "private templates." While such databases cannot be used for a background check, they are perfectly suitable for *one-to-one* access control systems or even for systems to prevent multiple registrations and related fraud. The user regains control over his or her sensitive information, such as medical or financial records, stored in the database.

Proliferation of BE technology may ultimately change the public's perception of biometrics. This would raise the benchmark for biometric technologies, such that the industry would be prompted to develop and adopt new privacy-friendly solutions. If the "private templates" generated by BE make a significant presence in the market, this could reshape the entire biometric industry. Increased user acceptance and confidence would be extremely beneficial for the industry.

Case Study #1: Small-scale use of Biometric Encryption

To demonstrate the power of BE, we will briefly present a biometric authentication protocol (remote or local) with third party certification. We use a simplified and reworded description from Boyen's paper on Fuzzy Extractors.[22]

Suppose that Alice wishes to authenticate herself to Bob using biometrics. Due to privacy concerns, she does not wish to reveal any biometric information to Bob. Conversely, for the authentication to be meaningful, Bob wants some assurance that Alice is in fact in possession of her purported biometrics at the time the authentication is taking place (i.e., that no one is impersonating her). We assume that there is a third party (often called the Trusted Authority), Trent, whom Bob trusts to honestly certify Alice's biometrics, and to whom Alice will temporarily grant access to her biometrics for the purpose of generating such a certificate. Alice will want to be able to obtain as many or as few of those certificates as she wants, and to reuse as many of them with multiple Bobs, some of whom may be even dishonest, without fear of privacy leaks or risk of impersonation. The protocol is as follows:

Enrolment and certification: Under Trent's supervision, and using Alice's own biometric:

1 Alice creates a Biometric Encryption template from her biometric and a randomly selected PIN. Neither the biometric nor the PIN can be recovered from the template;

2 The PIN is used to generate a pair of keys called *public* and *private keys*;

22 X. Boyen, "Reusable cryptographic fuzzy extractors," CCS 2004, pp. 82–91, ACM Press.

3 The biometric, the PIN, and the *private key* are discarded;

4 If Trent is satisfied that Alice has executed the steps honestly, he certifies the binding between Alice's name and the *public key*, i.e., he digitally signs the pair ["Alice," *public key*]. At this point, Alice may send the *public key* to Bob, or even publish it for all to see.

Verification: A challenge/response scheme is used to verify Alice:

1 At any time when appropriate (e.g. whenever Alice desires to authenticate herself to Bob), Bob sends Alice a fresh random challenge;

2 By obtaining her new biometric sample and applying it to her Biometric Encryption template, Alice recovers on-the-fly her PIN, which, in turn, regenerates her *private key*;

3 Alice signs the challenge with her *private key* and gives Bob the signature;

4 Bob authenticates Alice by checking the validity of the signature under her authentic *public key*.

The protocol does not require Alice to remember or store her PIN or her *private key*.

The Biometric Encryption template may be stored on a smart card or in Alice's laptop that also has a biometric sensor. For different applications ("multiple Bobs"), a new pair of *public* and *private keys* is generated from the PIN. Those keys are periodically updated. Some applications may require different PINs, in which case several Biometric Encryption templates can be stored. A proper template can be automatically recognized by the application.

The system based on digital signatures may be adopted both for a remote and local access. The important point is that the most critical part of any cryptosystem, the PIN (or a password), is securely bound to the biometrics.

In summary, Alice has in her possession and under her control as many BE templates as necessary. She can use them to digitally sign in, either for remote authentication or for logical or physical access. The authentication is done simply by checking the validity of her digital signature using standard cryptographic means. Neither Alice's biometric nor her PIN are stored or revealed. As a result, the system is both secure and highly privacy protective.

Case Study #2: Anonymous database; large or medium-scale applications

Suppose that a clinic, a hospital, or a network of hospitals maintains a database of medical records. Alice does not want her record to be accessed by unauthorized personnel or third parties, even for statistical purposes. For that the latter, her record is made anonymous and encrypted (by conventional means). The only public entry in the database is her personal identifier, which may be her real name or, in certain cases (e.g.

drug addiction clinic), an alias ("Jane Doe"). The link between Alice's identifier and her medical record is controlled by Biometric Encryption:

On enrolment, a BE template is created from Alice's biometric and a randomly generated PIN (Alice does not even know the PIN). The PIN is used to generate a pointer to Alice's medical record and a crypto-key that encrypts the record, and also a pair of keys called *public* and *private keys* (similar to case study 1). The BE template and the *public key* are associated with Alice's ID and stored in the database (they can be also stored on Alice's smart card); other temporary data, such as Alice's biometric, the PIN, the *private key*, the pointer, and the crypto-key, are discarded.

Suppose that Alice visits a doctor, to whom she wants to grant remote access to her medical record, or part of it, if the record is structured. From the doctor's office, Alice makes a request to the database administrator, Bob. The authentication procedure using challenge/response scheme is similar to that in case study 1:

1 If Alice does not have her smart card with her (e.g. in the case of an emergency), Bob sends Alice's BE template to the doctor's office;

2 Alice applies her new biometric sample to the BE template and recovers on-the-fly her PIN;

3 The PIN is used to regenerate her *private key*, the pointer to her medical record, and the crypto-key;

4 Bob sends Alice a fresh random challenge;

5 Alice signs the challenge with her *private key* and gives Bob the signature;

6 Bob authenticates Alice by checking the validity of the signature under her *public key*;

7 Alice securely sends Bob the pointer to her medical record;

8 Bob recovers Alice's encrypted medical record (or a part of it, also encrypted) and sends it to Alice;

9 Using her crypto-key, which was regenerated from her PIN, Alice decrypts her medical record for the doctor;

10 Alice's biometric, the PIN, the *private key*, the pointer, and the crypto-key, are discarded.

In summary, Bob (the database administrator) has an assurance that Alice is, in fact, who she claims to be (she was able to unlock her BE template in the doctor's office); he is also assured that her medical record was sent to the right person. On the other hand, Alice retains full control over her medical record, so that even Bob has no access to it, since he does not have the crypto-key to decrypt it. **The privacy protection is embedded into the system at a very basic technological level.**

Case Study #3: Travel documents; large-scale database applications

Using biometrics for travel documents has been a hot topic of discussion. To illustrate how BE can protect the user's privacy and, at the same time, improve the level of security, we will consider a re-worded description of a system proposed by Dr. van der Veen et al (Ref. [40] in Appendix 2).

The International Civil Aviation Organization (ICAO) dictates international standards for Machine Readable Travel Documents (MRTD), including those for ePassports. Among the recommendations is the "three-way-check" for secure verification at a border crossing. It involves comparing data originating from (i) the biometric sensor, (ii) the biometric image stored on the ePassport, and (iii) biometric data stored in external (centralized) databases.

BE technology provides the opportunity to do this in a privacy preserving manner: in addition to the biometric templates stored on the ePassport, their secure versions, namely, the BE templates, are also stored in a third-party database. The biometric images or conventional templates are not stored in the database. A "three-way check" is then performed by matching the BE template from the database to that appearing on the ePassport, and the live biometric measurement scanned at the kiosk. Border passage now involves the following steps:

1 At a kiosk, a user claims his identity (*ID*), and presents his biometric (e.g. facial image, fingerprint or iris) for measurements;

2 The *ID* is sent to the third-party database to extract the corresponding BE template;

3 The BE template is transmitted to the kiosk;

4 The BE template and the biometric measurement are combined to derive a cryptographic key, or rather a hashed version of it;

5 The image of the iris, face or fingerprint is extracted from the ePassport and used together with the BE template to derive another hashed version of the cryptographic key. This will validate the biometric stored on the ePassport;

6 Both hashed versions of the key derived on Steps 4 and 5 are transmitted to the border-control authority and verified against the database version. A positive authentication is achieved when all three versions are exactly the same.

In summary, the user's privacy is protected since the biometric image or template is not stored in a central database; instead, a secure BE template is stored. The database is inherently secure, meaning there is no need for complicated encryption and key management protocols. The ePassport is protected against tampering, since a potential attacker or any unauthorized user will not know the cryptographic key that was used to create the BE template.

Next Steps to Bringing Biometric Encryption to the Prototype Stage

Biometric Encryption has been researched since the mid-90s. Technologically, this area is much more challenging than conventional biometrics. But now, BE is fast approaching the next phase, i.e., the creation and testing of a prototype. The following issues still need to be addressed:

Select a Proper Biometric

The most promising results in terms of accuracy have been obtained for irises. Low variability of image samples, and the presence of a natural alignment feature (eye pupil) makes this biometric the number one candidate for BE.

Face recognition is the most publicly acceptable type of biometric. Recent advances in the technology allowed Philips Research to create the first operational BE system. At the present time, one of the drawbacks of the face-based BE system, however, is the relatively small size (~ 58 bits) of the encryption key that may be securely bound to the biometric.

Fingerprints, for which the BE was originally pioneered, are also a prime choice. The fingerprint biometrics used more widely than the iris or face, and most privacy concerns relate to fingerprints. On the other hand, using fingerprints for BE turns out to be much more challenging. The reasons are that high skin distortions can be introduced when the finger presses upon the sensor, and the difficulty of aligning a fingerprint on verification with the one enrolled. As mentioned before, the situation is more difficult for BE than for a conventional fingerprint verification, since BE works in a "blind" mode (the enrolled fingerprint or its minutiae template are not seen). Some of these issues can be overcome with a free-air image. Although this would present other optical issues, we believe they could be resolved by current technology. In general, face and especially iris are less vulnerable to distortion and alignment problems.[23]

Other biometrics, e.g. voice, signature, palmprints, etc., may not have enough entropy (i.e., the amount of non-redundant information to support a long enough cryptographic key). They could be possibly put on the list of "auxiliary" biometrics, i.e., used for BE in combination with irises, faces, or fingerprints or, perhaps, with conventional passwords (called "hardening").

Improve the Image Acquisition Process

For fingerprints, this means choosing a proper fingerprint sensor which is less susceptible to skin distortions (e.g. a free air sensor), or changing the existing sensor ergonomics to keep the distortions under control. Image quality can also be improved at the algorithm level (i.e., through software).

23 There have been independent tests, such as BioPII in Germany, that reported unusually high error rates for iris recognition: **www.bsi.de/literat/studien/biop/biopabschluss2.pdf**; **www.europeanbiometrics.info/images/resources/90_264_file.pdf**. Those results were questioned by Prof. John Daugman ("BioPII controversy to be tackled," Biometric Technology Today, vol. 13, no. 10, pp 1-2, 2005).

Make BE Resilient Against Attacks

This area of research, i.e., the analysis of potential vulnerability of BE against attacks, has been largely overlooked. By that we mean that a sophisticated attacker could gain access to both the BE templates and the algorithm. The only thing he cannot obtain is a user's biometric. Such an attacker, fully familiar with the algorithm and exploiting its weaknesses, will not be doing just a brute force search (i.e., about 2^{128} computations for a 128 bit key) in order to break the BE template. Instead, he will devise various attacks that can be run in a realistic time frame. The BE algorithm must be resilient against those off-line attacks. The same approach (i.e., resilience against attacks) is adopted in conventional cryptography.

Improve Accuracy and Security of BE Algorithm

There have been substantial advances in algorithm development in conventional biometrics in the past few years, as demonstrated by a series of international competitions. Many of those advances are applicable to BE.

Exploit Multimodal Approaches

This has been a hot area of research and development in conventional biometrics. The performance of a biometric system is significantly improved when different algorithms, or different fingers, or different biometrics (e.g. fingerprints and face) are combined. The modes that are combined should be "orthogonal," i.e., statistically independent. It is reasonable to expect that the multimodal approach would work also for BE.

Develop BE Applications

The applications, such as those described in the case studies, should clearly demonstrate the benefits for privacy and security brought about by the use of BE.

Summary and Conclusions

Biometric Encryption technology is a fruitful area for research and has become sufficiently mature for broader public policy consideration, prototype development, and consideration of applications.

This paper has explored the possibilities and privacy-enhancing benefits of Biometric Encryption technologies for meeting the needs of businesses and government agencies.

We believe that BE technology exemplifies fundamental privacy and data protection principles that are endorsed around the world, such as data minimization, user empowerment and security, better than any other biometric technology solution in existence.

We hope that our paper will form a valuable contribution to current national and international discussions regarding the most appropriate methods to achieve, in a privacy-enhanced manner, strong identification and authentication protocols.

While introducing biometrics into information systems may result in considerable benefits, it can also introduce many new security and privacy vulnerabilities, risks, and concerns, as discussed above. However, novel Biometric Encryption techniques have been developed that can overcome many, if not most, of those risks and vulnerabilities, resulting in a win-win, positive-sum scenario.

One can only hope that the biometric portion of such systems is done well, and preferably not modelled on a zero-sum paradigm, where there must always be a winner and a loser. A positive-sum model, in the form of Biometric Encryption, presents distinct advantages to both security AND privacy.

Appendices

For the two extensive appendices, please see the online version of *Biometric Encryption: A Positive Sum Technology that Achieves Strong Authentication, Security AND Privacy* at **www.ipc.on.ca**.

About The Authors

Ann Cavoukian, Ph.D.
Information and Privacy Commissioner of Ontario, Dr. Ann Cavoukian, is recognized as one of the leading privacy experts in the world and the published author of two groundbreaking books on privacy – *Who Knows: Safeguarding Your Privacy in a Networked World* (1997), written with Don Tapscott, and *The Privacy Payoff: How Successful Businesses Build Customer Trust* (2002), written with Tyler Hamilton. Overseeing the operations of the access and privacy laws in Canada's most populous province, Commissioner Cavoukian serves as an Officer of the Legislature, independent of the government of the day.

Alex Stoianov, Ph.D.
Dr. Alex Stoianov began working in the field of biometrics after joining Mytec Technologies Inc. (Toronto, Canada) in 1994 where he was one of the originators of the privacy-enhancing technology, Biometric Encryption. Working for Bioscrypt Inc., the successor of Mytec, as a Principal Scientist from 2001 to 2006, he developed numerous technological breakthroughs and improvements for fingerprint verification algorithms. He also won the Third International Fingerprint Verification Competition (FVC2004), viewed by many as the "Fingerprint Olympics," on the company's behalf. Dr. Stoianov has co-authored over 30 scientific papers and seven patents.

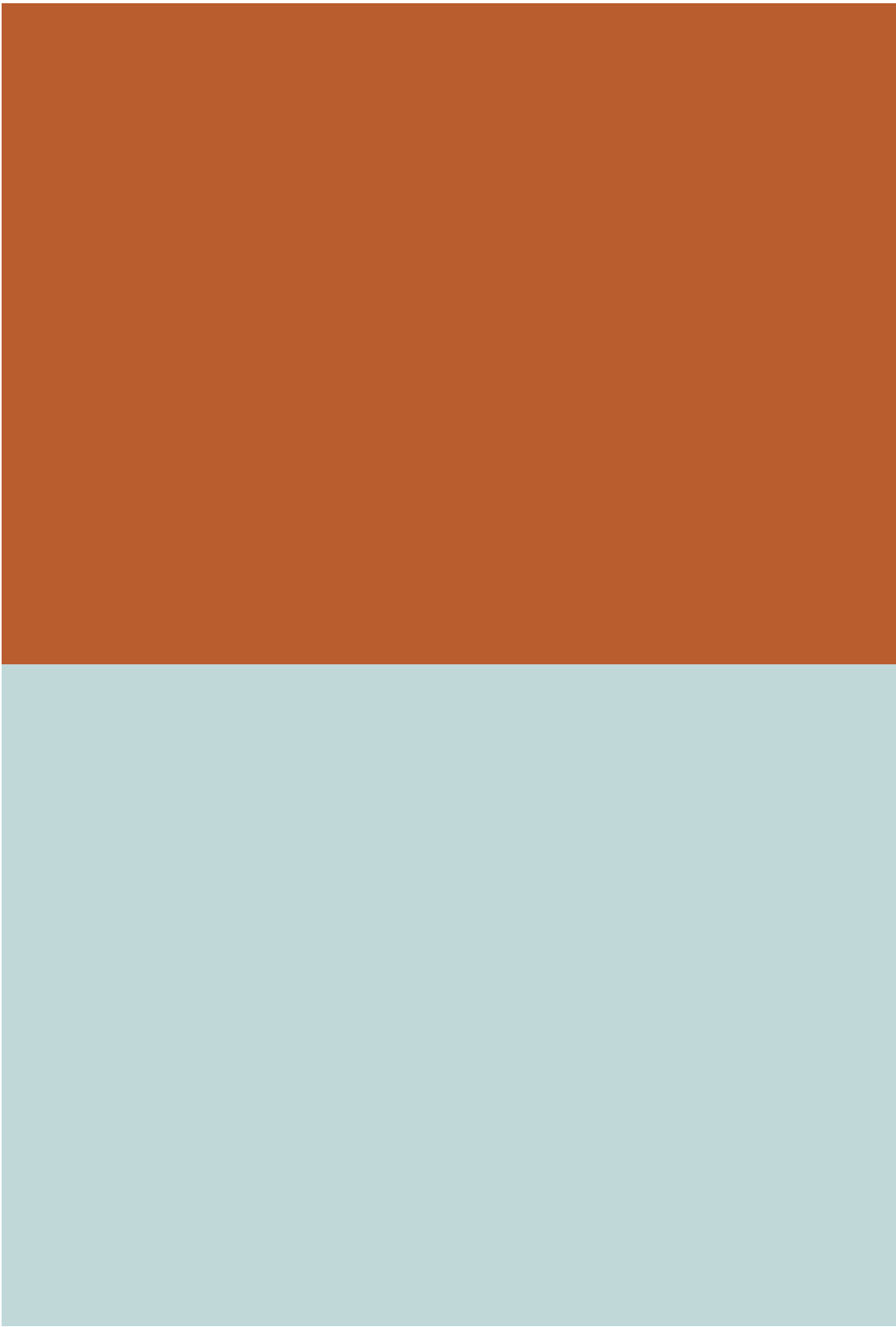
The authors gratefully acknowledge the work of Fred Carter, IPC Senior Policy and Technology Advisor, in the preparation of this paper.

The authors would also like to thank Prof. Dr. Christoph Busch, of Fraunhofer IGD, Germany, and Mr Bernard Didier and Mme Alexandra Michy, both of Sagem Défense Sécurité, France, for their review and contributions to the pre-publication draft.

In addition, we would like to thank Dr. Michiel van der Veen, Senior Manager, Business Development Biometrics, Phillips Research, of the Netherlands, for bringing to our attention their recent white paper, *privID™: Privacy Protection in Biometric Security Applications*, and to the fact that Phillips now has biometric encryption applications that are operational and ready for deployment.

Creation of a Global Privacy Standard

November 2006



Introduction

In 2005, at the 27th International Data Protection Commissioners Conference in Montreux, Switzerland, I chaired a Working Group of Commissioners. This Working Group was convened for the sole purpose of creating a single Global Privacy Standard. Faced with globalization and convergence of business practices, regardless of borders, I thought there was a pressing need to harmonize various sets of fair information practices into one Global Privacy Standard. Once such a foundational policy piece was in place, then businesses and technology companies could turn to a single instrument for evaluating whether their practices or systems were actually privacy enhancing, in nature and substance.

While attempting to develop a single law on data protection was beyond our reach, I was confident that we could develop a single privacy instrument, globally. In advancing my objective to develop a harmonized set of fair information practices, my office embarked on the preliminary work of conducting a "Gap Analysis." This was the process of comparing leading privacy practices and codes from around the world, comparing their various attributes, and the scope of the privacy principles enumerated therein. We identified the strengths and weaknesses of the major codes in existence and then tabled our Gap Analysis with the Working Group of Commissioners.

In the months that ensued, we embarked upon the work of harmonizing the principles into a single set of fair information practices. This led to the development of the attached Global Privacy Standard (GPS), which builds upon the strengths of existing codes containing time-honoured privacy principles and, for the first time, reflects a noteworthy enhancement by explicitly recognizing the concept of "data minimization" under the "collection limitation" principle.

After successive drafts of the GPS were developed, revised and circulated for review, the attached final version of the GPS was formally tabled and accepted in the United Kingdom, on November 3, 2006, at the 28th International Data Protection Commissioners Conference.

Objective

The objective of the Global Privacy Standard is to form a set of universal privacy principles, harmonizing those found in various sets of fair information practices presently in existence.

The Global Privacy Standard draws upon the collective knowledge and practical wisdom of the international data protection community.

Scope

The Global Privacy Standard reinforces the mandate of privacy and data protection authorities by:

- focusing attention on fundamental and universal privacy concepts;
- widening current privacy awareness and understanding;
- stimulating public discussion of the effects of new information and communication technologies, systems, standards, social norms, and laws, on privacy; and
- encouraging ways to mitigate threats to privacy.

The GPS informs developers and users of new technologies and systems that manage or process information. The GPS may be particularly useful when developing information and communication technology standards, specifications, protocols, and associated conformity assessment practices.

The GPS can assist public policy-makers when considering laws, regulations, programs and the use of technologies that may impact privacy. The GPS can equally assist businesses and developers of technology that may have an impact on privacy and personal information.

The GPS addresses privacy concerns for decision-makers in any organization that has an impact on the way in which personal information is collected, used, retained, and disclosed.

The GPS is not intended to pre-empt or contradict any other laws or legal requirements bearing upon privacy and personal information in various jurisdictions.

GPS Privacy Principles

1 **Consent:** The individual's free and specific consent is required for the collection, use or disclosure of personal information, except where otherwise permitted by law. The greater the sensitivity of the data, the clearer and more specific the quality of the consent required. Consent may be withdrawn at a later date.

2 **Accountability:** Collection of personal information entails a duty of care for its protection. Responsibility for all privacy related policies and procedures shall be documented and communicated as appropriate, and assigned to a specified individual within the organization. When transferring personal information to third parties, organizations shall seek equivalent privacy protection through contractual or other means.

3 **Purposes:** An organization shall specify the purposes for which personal information is collected, used, retained and disclosed, and communicate these purposes to the individual at or before the time the information is collected. Specified purposes should be clear, limited and relevant to the circumstances.

4 **Collection Limitation:** The collection of personal information must be fair, lawful and limited to that which is necessary for the specified purposes.

> **Data Minimization** – The collection of personal information should be kept to a strict minimum. The design of programs, information technologies, and systems should begin with non-identifiable interactions and transactions as the default. Wherever possible, identifiability, observability, and linkability of personal information should be minimized.

5 **Use, Retention, and Disclosure Limitation:** Organizations shall limit the use, retention, and disclosure of personal information to the relevant purposes identified to the individual, except where otherwise required by law. Personal information shall be retained only as long as necessary to fulfil the stated purposes, and then securely destroyed.

6 **Accuracy:** Organizations shall ensure that personal information is as accurate, complete, and up-to-date as is necessary to fulfil the specified purposes.

7 **Security:** Organizations must assume responsibility for the security of personal information throughout its lifecycle consistent with the international standards that have been developed by recognized standards development organizations. Personal information shall be protected by reasonable safeguards, appropriate to the sensitivity of the information (including physical, technical and administrative means).

8 **Openness:** Openness and transparency are key to accountability. Information about the policies and practices relating to the management of personal information shall be made readily available to individuals.

9 **Access:** Individuals shall be provided access to their personal information and informed of its uses and disclosures. Individuals shall be able to challenge the accuracy and completeness of the information and have it amended as appropriate.

10 **Compliance:** Organizations must establish complaint and redress mechanisms, and communicate information about them to the public, including how to access the next level of appeal. Organizations shall take the necessary steps to monitor, evaluate, and verify compliance with their privacy policies and procedures.

7 Laws Of Identity: The Case For Privacy-Embedded Laws Of Identity

October 2006

Backdrop

The existing identity infrastructure of the Internet is no longer sustainable. The level of fraudulent activity online has grown exponentially over the years and is now threatening to cripple e-commerce. Something must be done now before consumer confidence and trust in online activities are so diminished as to lead to its demise. Enter the 7 Laws of Identity: could this be the answer? Read on.

— Ann Cavoukian, Ph.D.
Information and Privacy Commissioner of Ontario

Introduction

This paper recognizes and is inspired by the "7 Laws of Identity" formulated on an open blog by a global community of experts through the leadership of Kim Cameron, Chief Identity Architect at Microsoft.

The Office of the Information and Privacy Commissioner of Ontario is convinced that the "7 Laws" (*a.k.a.* "technologically-necessary principles of identity management") will profoundly shape the architecture and growth of a universal identity metasystem. The resulting "Identity Big Bang" will hopefully enable the Internet to evolve to the next level of trust and capability.

A universal identity metasystem will also have profound impacts on privacy since the digital identities of people – and the devices associated with them – constitute personal information. Care must be taken that a universal, interoperable identity metasystem does not get distorted and become an infrastructure of universal surveillance.

We have always advocated that privacy be built into the design and operation of information systems and technologies. We do this by applying the privacy principles expressed in the "Fair Information Practices" in a systematic way. (See Appendix A)

We are struck by the many similarities between the 7 Laws of Identity and the fair information practices. The two sets of fundamental principles are highly complementary and inform each other.

This document is the result of our "mapping" fair information practices over the 7 Laws of Identity to explicitly extract their privacy-protective features. The result, which we call the "privacy-embedded" Laws of Identity, is a commentary on the Laws that "teases-out" the privacy implications, for all to consider.

The privacy-embedded Laws of Identity are intended to inject privacy considerations into discussions involving identity – specifically, into the emerging technologies that will define an interoperable identity system.

We believe that privacy is woven through the 7 Laws and that when the Laws are applied, exciting new privacy options will become possible. However, there is nothing inevitable about privacy-enhanced identification and authentication options. An identity metasystem (described by the 7 Laws) is a necessary but not sufficient condition for privacy-enhancing options to be developed.

The missing ingredients are knowledge and desire. If privacy design options for identity systems can be identified and promoted, then it is possible that a universal identity metasystem will emerge that has built-in respect for privacy and data protection, before it's too late.

Identity and Privacy

Identity and privacy are closely related. Generally speaking, when your identity is not known, you tend to have more privacy. When you pay cash for a coffee, your "identity" is that of an anonymous consumer. When you buy coffee with an anonymous pre-paid coffee card, your "identity" becomes that of a loyal patron. But, when your name and address are linked to a pre-paid coffee card, all of your coffee purchases may be linked to you, as an identifiable individual. Information that can be linked to an identifiable individual is considered to be personal information.

Privacy refers to the claim or right of individuals to exercise a measure of control over the collection, use and disclosure of their personal information. When your personal information is mishandled, your privacy interests are engaged.

Protecting and promoting individual privacy is a real challenge in an era of exponential creation, networking and duplication of data, most of which is identifiable in nature. There is more personal information out there than ever before, and most of it is controlled by others. Increasingly we have little control over our own information.

Identification requirements are everywhere, and increasing. We all have multiple identities which need to be managed. In the online digital environment, however, the identity challenges are greater, since identification demands are becoming more frequent. Increasingly, more and more granular information is being collected about us by others, and this data is being used in novel ways, for novel purposes – not all of which benefit the individual.

There is a growing disjunct with the bricks-and-mortar world where, for example, we can often demonstrate our identity (or credentials) by simply waving an ID document for visual inspection. But in the faceless online world, our identification "credential" is often recorded in databases, compared or collated with other data, and stored indefinitely for further uses.

At the same time, the identity of other entities online is becoming harder to verify. We often simply do not know who we are truly dealing with online, or how accountable they are with respect to the handling of our personal information.

Digital Identity and Privacy: The Challenge

For users and businesses alike, the Internet continues to be increasingly valuable. More people are using the web for everyday tasks, from shopping, banking, and paying bills to consuming media and entertainment. E-commerce opportunities are growing, with businesses delivering more services and content across the Internet, communicating and collaborating online, and inventing new ways to connect with each other.

But as the value of what people do online has increased, the Internet itself has become more complex, vulnerable, and dangerous. Online identity theft, fraud, and privacy concerns are on the rise, stemming from increasingly sophisticated practices such as "phishing," "spear-phishing," and "pharming." Keeping track of multiple accounts, passwords and authentication methods is difficult and frustrating for users. "Password fatigue" results in insecure practices such as re-using the same account names and passwords at many sites.

The Need for Identity Management

Identity management is a hot topic these days, but what exactly is it? The term does not have a clearly defined meaning, but technology-based identity management, in its broadest sense, refers to the administration and design of identity attributes, credentials, and privileges.

Identity management may be carried out centrally by others, as in the case of organizations that assign "log on" credentials to individuals to facilitate and control access to critical resources. When you leave the organization, your network identity and associated privileges are revoked by the system administrator. This is often called *enterprise* identity management or, more simply, *provisioning*. Centralized identity management may also occur beyond the enterprise, as when governments issue national identity cards for use in multiple scenarios, or in some online single-sign-on schemes such as Microsoft .Net Passport service.

Another form of identity management is "user-centric" which seeks to place administration and control of identity information directly into the hands of individuals. Examples include network anonymization tools and form fillers that minimize disclosure of personal information, or password managers that securely keep track of different credentials. In the real world, a wallet full of different identity cards is a user-centric form of identity management that allows individuals to choose the appropriate identity credential for the right purposes, such as a coffee card for coffee and a student ID card for discounts. Individuals can exercise control over how the information on those cards is read and used by others.

A third type of identity management, commonly referred to as "federated," is a hybrid of the two. In such systems, one's identity credentials are divided and spread out among many parties, with users controlling how they are shared and used. Some single sign-on schemes can work this way. The ability to authorize a government agency to share change-of-address information with other departments may be another. The

risks to privacy can be offset by careful choice of trusted identity providers, and by greater convenience and efficiencies for users.

All three types of identity management systems are necessary, depending on the context. Identity is highly contextual. Consider that the identities held by a person in the offline world can range from the significant, such as birth certificates, passports, and drivers' licenses, to the trivial, such as business cards or frequent user buyer's cards. People use their different forms of identification in different contexts where they are accepted.

Identity is Contextual

Personal information provided in different contexts will vary. Identities may be used in or out of context. Identities used out of context generally do not bring desired results. For example, trying to use a coffee card to cross a border is clearly out of context. On the other hand, using a bank card at an ATM, a government-issued ID at a border, a coffee card at a coffee shop, and a MS.Net Passport account at MSN Hotmail are all clearly in context.

In some cases, the distinction is less clear. You could conceivably use a government-issued ID at your ATM instead of a bank-issued card, but if this resulted in the government having knowledge of each financial transaction, many people would be uncomfortable. You could use a Social Insurance or Social Security Number as a student ID number, but that has significant privacy implications, such as facilitating identity theft. And you can use a .Net Passport account at some non-Microsoft sites, but few sites chose to enable this; even where it was enabled, few users did so because they felt that Microsoft's participation in these interactions was out of context.

Numerous digital identity systems have been introduced, each with its own strengths and weaknesses. But no one single system meets the needs of every digital identity scenario. Even if it were possible to create one system that did so, the reality is that many different identity systems are in use today, with still more being invented. As a result, the current state of digital identity on the Internet is an inconsistent patchwork of ad hoc solutions that burdens people with different user experiences at every web site, renders the system as a whole fragile, and constrains the fuller realization of the promise of e-commerce.

The Internet's Problems are often Identity Problems

Many of the problems facing the Internet today stem from the lack of a widely deployed, easily understood, secure identity solution.

A comparison between the bricks-and-mortar world and the online world is illustrative: In the bricks-and-mortar world you can tell when you are at a branch of your bank. It would be very difficult to set up a fake bank branch and convince people to do transactions there. But in today's online world it is trivial to set up a fake banking site (or e-commerce site …) and convince a significant portion of the population that it's the real thing. This is an enormous identity problem. Web sites currently do not have reliable

ways of identifying themselves to people, thus enabling impostors to flourish. What is needed is reliable *site-to-user* authentication, which aims to make it as difficult to produce counterfeit services in the online world, as it is to produce them in the physical world.

Conversely, problems identifying users to sites also abound. Username/password authentication is the prevailing paradigm, but its weaknesses are all too evident on today's Internet. Password re-use, insecure passwords, and poor password management practices open a world of attacks, in and of themselves. Combine that with the password theft attacks enabled by counterfeit web sites, and man-in-the-middle attacks, and today's Internet is an attacker's paradise.

The consequences of these problems are severe and growing. The number of "phishing" attacks and sites has skyrocketed. There are reports that online banking activity is declining. Recent regulatory guidance on authentication in online banking reports that "Account fraud and identity theft are frequently the result of single-factor (e.g., ID/password) authentication exploitation." [FFIEC 05] Consumer trust of the Internet is low and ever-dropping.[NCL 06] Clearly, the status quo is no longer a viable option.

What is Needed: an Identity Metasystem

Given that universal adoption of a single digital identity system or technology is unlikely to occur, a successful and widely deployed identity solution for the Internet requires a different approach – one with the capability to connect existing and future identity systems into an **identity metasystem**. A metasystem, or system of systems, would leverage the strengths of its constituent identity systems, provide interoperability between them, and enable the creation of a consistent and straightforward user interface to all of them. The resulting improvements in cyberspace would benefit everyone, ultimately making the Internet a safer place with the potential to boost e-commerce, combat phishing, and solve other digital identity challenges.

An identity metasystem could make it easier for users to stay safe and in control when accessing resources on the Internet. It could allow users to select from among a portfolio of their digital identities and use them for Internet services of their choice, where they are accepted. A metasystem could enable identities provided by one identity system technology to be used within systems based on different technologies, provided that an intermediary exists that understands both technologies and is capable and trusted to do the needed translations.

It is important to note that the role of an identity metasystem is not to compete with or replace the identity systems that it connects. Rather, a metasystem should rely on the individual systems in play to do its work!

Architecture of a Proposed Solution

By definition, in order for a digital identity solution to be successful, it needs to be understood in all the contexts when you may wish to use it to identify yourself. Identity systems are all about identifying yourself (and your things) in environments that are not

yours. For this to be possible, both your systems and the systems that are not yours – those where you need to digitally identify yourself – must be able to speak the same digital identity protocols, even if they are running different software on different platforms.

Such a solution, in the form of an identity metasystem, has already been proposed, and some implementations are well under way. The identity metasystem is based upon an underlying set of principles called the "Laws of Identity." The Laws are intended to codify a set of fundamental principles to which a universally adopted, sustainable identity architecture must conform. The Laws were proposed, debated, and refined through a long-running, open, and continuing dialogue on the Internet by the major players in the identity field. Taken together, the Laws are key to defining the overall architecture of the identity metasystem.

Because these Laws were developed through an open consensus process among experts and stakeholders, they reflect a remarkable convergence of interests, and are non-proprietary in nature. As a result, they have been endorsed and adopted by a long and growing list of industry organizations, associations, and technology developers.

By allowing different identity systems to work together in concert, with a single user experience, and a unified programming paradigm, the metasystem shields users and developers from concerns about the evolution and market dominance of specific underlying systems, thereby reducing everyone's risk and increasing the speed with which the technology can evolve.

It is our sincere belief that the 7 Laws of Identity and the identity metasystem they describe represent significant contributions to improving security and privacy in the online world and, as such, are worthy of closer study, support and broad adoption by the privacy community.

We are particularly struck by the parallels with the fair information practices ("FIPs"), which set forth universal principles that both establish and confer broad rights on *individuals* with respect to the collection, use, and disclosure of their personal information by others, and at the same time set out broad responsibilities for *organizations* in respect to their collection, use and disclosure of personal information. The FIPs have served as the basis for privacy and data protection laws around the world, and yet are versatile enough to be used to guide the design, development and operation of information technologies and systems in a privacy-enhancing manner.

We are impressed with how the Laws of Identity seek to put users in control of their own identities, their personal information, and their online experiences. In the metasystem, users decide how much information they wish to disclose, to whom, and under what circumstances, thereby enabling them to better protect their privacy. Strong two-way authentication of identity providers and relying parties helps address phishing and other forms of fraud. Identities and accompanying personal information can be securely stored and managed in a variety of ways, including via the online identity provider

service of the user's choice, or on the user's PC, or in other devices such as secure USB keychain storage devices, smartcards, PDAs, and mobile phones.

Further, the identity metasystem enables a predictable, uniform user experience across multiple identity systems. It extends to and integrates the human user, thereby helping to secure the machine-human channel.

Participants in the identity metasystem may include anyone or anything that uses, participates in, or relies upon identities in any way, including, but not limited to existing identity systems, corporate identities, government identities, Liberty federations, operating systems, mobile devices, online services, and smartcards. Again, the possibilities are only limited by innovators' imaginations.

An example of a universal identity system that did NOT conform with the Laws of Identity is illustrative.

.Net Passport

Until now, Microsoft's best-known identity effort was almost certainly the Passport Network, best known to millions of Internet users as a "single sign-on" identity system that stored users' personal information centrally.

The identity metasystem is different from the original version of Passport in several fundamental ways. The metasystem stores no personal information, leaving it up to individual identity providers to decide how and where to store that information. The identity metasystem is not an online identity provider for the Internet; indeed, it provides a means for all identity providers to co-exist with and compete with one another – all having equal standing within the metasystem. And while Microsoft charged companies to use the original version of Passport, no one will be charged to participate in the identity metasystem.

In fairness, the Passport system itself has evolved in response to these experiences. It no longer stores personal information other than username/password credentials. Passport is now an authentication system targeted at Microsoft sites and those of close partners – a role that is clearly in context, and one which users and partners are more comfortable. Passport and MSN plan to implement support for the identity metasystem as an online identity provider for MSN and its partners. Passport users will receive improved security and ease of use, and MSN Online partners will be able to interoperate with Passport through the identity metasystem.

An example of one desktop application, currently in development, that does embody the 7 Laws of the identity metasystem is also illustrative.

Cardspace and Information Cards

Microsoft, among others, is building user software that conforms to the 7 Laws of the identity metasystem. The "Cardspace" identity selector is a Windows component that provides the consistent user experience required by the identity metasystem. It is specifically hardened against tampering and spoofing to protect the end user's digital

identities and maintain end-user control. Each digital identity managed in Cardspace (comparable to a virtual card holder) is represented by a visual “information card” in the user interface. The user selects identities represented by information cards to authenticate to participating services.

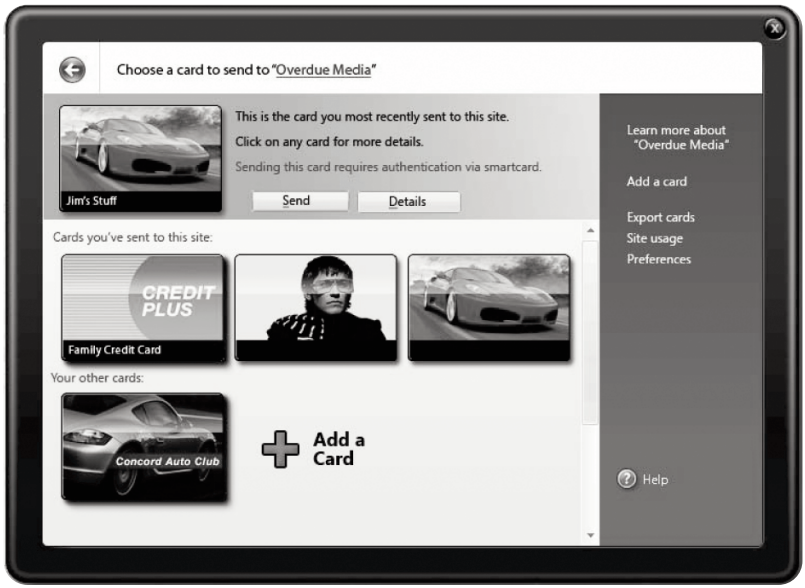


Figure 1: Identity Selector Screen: Information Cards

Many identity attacks succeed because the user was fooled by something presented on the screen, not because of insecure communication technologies. For example, phishing attacks occur not in the secured channel between web servers and browsers — a channel that might extend thousands of miles — but in the two or three feet between the browser and the human who uses it. The identity metasystem, therefore, seeks to empower users to make informed and reasonable identity decisions by enabling the use of a consistent, comprehensible, and self-explanatory user interface for making those choices.

As Figure 1 illustrates, users can be in control of their identity interactions (see Laws 1 & 2) by being able to choose which identities to use at which services, by knowing what information will be disclosed to those services if they use them, and by being informed how those services will use the information they disclose. To be in control, you must first be able to understand the choices you are presented with (see Laws 6 & 7). Unless users can be brought into the identity solution as informed, functioning components of the solution, able to consistently make good choices on their own behalf, the problem will not be solved.

Information cards have several key advantages over username/password credentials:

- **No weak, reused, lost, forgotten or stolen credentials:** Because no password is typed in or sent, passwords cannot be stolen or forgotten.
- **Better site authentication; less phishing:** Because authentication can be based on unique keys generated for every information card/site pair, the keys known by one site are useless for authentication purposes at another, even for the same information card. This directly addresses the phishing and fake website problems.
- **Data Minimization:** Because information cards can re-supply identity information or claim values (e.g., name, address, and e-mail address) to other sites with whom they are dealing, those sites don't need to store this data between sessions. Retaining less data, or data minimization, means that sites have fewer vulnerabilities. (See Law 2.)
- **Consistent Interface = Better choices:** Programs like Cardspace implement a standard user interface for working with digital identities. Perhaps the most important part of this interface, the screen used to select an identity to present to a site, is shown in the Figure above.

There are many information card systems. It is worth noting that, by extending the "real-world" visual metaphors and cues of the wallet containing various cards and credentials, information card software such as that by Microsoft makes it possible for users to be in better control of their digital identities. We encourage interested readers to read the seminal whitepapers freely available at **www.identityblog.com** which further explain and clarify the Laws of Identity and information cards in greater detail.

Let us now turn to the privacy features embedded in the identity metasystem.

Privacy Analysis and Commentary on the 7 Laws of Identity

In light of the preceding discussion and the identity challenges and opportunities that lie ahead, we carried out the following privacy analysis and commentary on the 7 Laws of Identity (and, by extension, on the identity metasystem that those laws collectively describe).

The following chart is the summary result of our efforts to "map" fair information practices to the Laws of Identity, in order to explicitly extract their privacy-protective features. The result is a commentary on the Laws that "teases-out" their privacy implications, for all to consider.

In brief, the privacy-embedded Laws of Identity, when implemented, offer individuals:

- easier and more direct user control over their personal information when online;
- enhanced user ability to minimize the amount of identifying data revealed online;
- enhanced user ability to minimize the linkage between different identities and actions;
- enhanced user ability to detect fraudulent messages and websites, thereby minimizing the incidence of phishing and pharming.

Laws of Identity

The 7 Laws of Identity	7 Privacy-Embedded Laws of Identity
Law #1: User Control and Consent	**Law #1:** Personal Control and Consent
Technical identity systems must only reveal information identifying a user with the user's consent.	Technical identity systems must only reveal information identifying a user with the user's consent. Personal control is fundamental to privacy, as is freedom of choice. Consent is pivotal to both. *Consent must be invoked in the collection, use and disclosure of one's personal information. Consent must be informed and uncoerced, and may be revoked at a later date.*
Law #2: Minimal Disclosure for a Constrained Use	**Law #2:** Minimal Disclosure for Limited Use: Data Minimization
The identity metasystem must disclose the least identifying information possible, as this is the most stable, long-term solution.	The identity metasystem must disclose the least identifying information possible, as this is the most stable, long-term solution. It is also the most privacy protective solution. *The concept of placing limitations on the collection, use and disclosure of personal information is at the heart of privacy protection. To achieve these objectives, one must first specify the purpose of the collection and then limit one's use of the information to that purpose. These limitations also restrict disclosure to the primary purpose specified, avoiding disclosure for secondary uses. The concept of data minimization bears directly upon these issues, namely, minimizing the collection of personal information in the first instance, thus avoiding the possibility of subsequent misuse through unauthorized secondary uses.*
Law #3: Justifiable Parties	**Law #3:** Justifiable Parties: "Need to Know" Access
Identity systems must be designed so the disclosure of identifying information is limited to parties having a necessary and justifiable place in a given identity relationship.	Identity systems must be designed so the disclosure of identifying information is limited to parties having a necessary and justifiable place in a given identity relationship. This is consistent with placing limitations on the disclosure of personal information, and only allowing access on a "need-to-know" basis. *Only those parties authorized to access the data, because they are justifiably required to do so, are granted access.*

The 7 Laws of Identity	7 Privacy-Embedded Laws of Identity
Law #4: Directed Identity	**Law #4:** Directed Identity: Protection and Accountability
A universal identity metasystem must support both "omnidirectional" identifiers for use by public entities and "unidirectional" identifiers for use by private entities, thus facilitating discovery while preventing unnecessary release of correlation handles.	A universal identity metasystem must be capable of supporting a range of identifiers with varying degrees of observability and privacy. Unidirectional identifiers are used by the user exclusively for the other party, and support an individual's right to minimize data linkage across different sites. This is consistent with privacy principles that place limitations on the use and disclosure of one's personal information. At the same time, users must also be able to make use of omnidirectional identifiers provided by public entities in order to confirm who they are dealing with online and, thereby ensure that that their personal information is being disclosed appropriately. To further promote openness and accountability in business practices, other types of identifiers may be necessary to allow for appropriate oversight through the creation of audit trails.
Law #5: Pluralism of Operators and Technologies	**Law #5:** Pluralism of Operators and Technologies: Minimizing Surveillance
A universal identity solution must utilize and enable the interoperation of multiple identity technologies run by multiple identity providers.	The interoperability of different identity technologies and their providers must be enabled by a universal identity metasystem. Both the interoperability and segregation of identity technologies may offer users more choices and control over the means of identification across different contexts. In turn, this may minimize unwanted tracking and profiling of personal information obtained through surveillance of visits across various sites.
Law #6: Human Integration	**Law #6:** The Human Face: Understanding is Key
The identity metasystem must define the human user to be a component of the distributed system, integrated through unambiguous human-machine communication mechanisms offering protection against identity attacks.	Users must figure prominently in any system, integrated through clear human-machine communications, offering strong protection against identity attacks. This will advance user control, but only if users truly understand. Thus, plain language in all communications used to interface with individuals is key to understanding. Trust is predicated on such understanding.
Law #7: Consistent Experience across Contexts	**Law #7:** Consistent Experience across Contexts: Enhanced User Empowerment and Control
The unifying identity metasystem must guarantee its users a simple, consistent experience while enabling separation of contexts through multiple operators and technologies.	The unifying identity metasystem must guarantee its users a simple, consistent experience while enabling separation of contexts through multiple operators and technologies. We return full circle to the concept of individual empowerment and informed consent. Clear interfaces, controls and options that enhance an individual's ability to exercise control across multiple contexts in a reliable, consistent manner will serve to enhance the principle of informed consent.

Conclusions

The Internet was built without a way to know who and what individuals are communicating with. This limits what people can do and exposes computer users to potential fraud. If nothing is done, the result will be rapidly proliferating episodes of theft and deception that will cumulatively erode public trust. That confidence is already eroding as a result of spam, phishing, pharming and identity theft, which leaves online consumers vulnerable to the misuse of their personal information and minimizes the future potential of e-commerce. The privacy-embedded 7 Laws of Identity supports the global initiative to empower consumers to manage their own digital identities and personal information in a much more secure, verifiable and private manner.

Identity systems that are consistent with the privacy-embedded 7 Laws of Identity will help consumers verify the identity of legitimate organizations before they decide to continue with an online transaction. Consumers today are being spammed, phished, pharmed, hacked and otherwise defrauded out of their personal information in alarming numbers, in large part because there are few reliable ways for them to distinguish the “good guys” from the “bad.”

E-commerce providers are taking note of this trend because declining consumer confidence and trust are especially bad for business. The next generation of intelligent and interactive web services (“Web 2.0”) will require more, not fewer, verifiable identity credentials, and much greater mutual trust in order to succeed.

Just as the Internet emerged from connecting different proprietary networks, an “Identity Big Bang” is expected to happen once an open, non-proprietary and universal method to connect identity systems and ensure user privacy is developed, in accordance with universal privacy principles. Already, there is a long and growing list of companies and individuals that endorse the 7 Laws of Identity and are working towards developing identity systems that conform to them. Participants include e-commerce sites, financial institutions, governments, Internet service providers, mobile telephony operators, certificate authorities, and software vendors for a broad range of platforms.

Our efforts to describe the 7 privacy-embedded Laws of Identity are intended to inject privacy considerations into discussions involving identity – specifically, into the emerging technologies that will define an interoperable identity system. We hope that our commentary will stimulate broader discussion across the Internet blogosphere and among the “identerati.”

We also hope that software developers, the privacy community and public policy-makers will consider the 7 privacy-embedded Laws of Identity closely, discuss them publicly, and take them to heart. Promoting privacy-enhanced identity solutions at a critical time in the development of the Internet and e-commerce will enable both privacy and identity to be more strongly protected.

APPENDIX A: Fair Information Practices

CSA Privacy Code

Principles in Summary

Ten interrelated principles form the basis of the CSA Model Code for the Protection of Personal Information. Each principle must be read in conjunction with the accompanying commentary.

1 **Accountability:** An organization is responsible for personal information under its control and shall designate an individual or individuals who are accountable for the organization's compliance with the following principles.

2 **Identifying Purposes:** The purposes for which personal information is collected shall be identified by the organization at or before the time the information is collected.

3 **Consent:** The knowledge and consent of the individual are required for the collection, use, or disclosure of personal information, except where inappropriate.

4 **Limiting Collection:** The collection of personal information shall be limited to that which is necessary for the purposes identified by the organization. Information shall be collected by fair and lawful means.

5 **Limiting Use, Disclosure, and Retention:** Personal information shall not be used or disclosed for purposes other than those for which it was collected, except with the consent of the individual or as required by law. Personal information shall be retained only as long as necessary for the fulfilment of those purposes.

6 **Accuracy:** Personal information shall be as accurate, complete, and up-to-date as is necessary for the purposes for which it is to be used.

7 **Safeguards:** Personal information shall be protected by security safeguards appropriate to the sensitivity of the information.

8 **Openness:** An organization shall make readily available to individuals specific information about its policies and practices relating to the management of personal information.

9 **Individual Access:** Upon request, an individual shall be informed of the existence, use, and disclosure of his or her personal information and shall be given access to that information. An individual shall be able to challenge the accuracy and completeness of the information and have it amended as appropriate.

10 **Challenging Compliance:** An individual shall be able to address a challenge concerning compliance with the above principles to the designated individual or individuals accountable for the organization's compliance.

Source: www.csa.ca/standards/privacy

APPENDIX B: Information Sources and Other Useful Reading Materials

The Case for Privacy-Embedded Laws of Identity in the Digital Age
Identity Theft Revisited: Security is Not Enough
www.ipc.on.ca

Kim Cameron's Identity Weblog
www.identityblog.com

The LAWS OF IDENTITY
An introduction to Digital Identity - the missing layer of the Internet
www.identityblog.com/?page_id=354

The IDENTITY METASYSTEM
A proposal for building an identity layer for the Internet
www.identityblog.com/?page_id=355

Identity Management Research & Development Projects

- InfoCard / CardSpace: **www.identityblog.com/wp-content/resources/design_rationale.pdf**
- Open Source identity Selector (OSIS) project: **http://osis.netmesh.org**
- Shibboleth: **http://shibboleth.internet2.edu/about.html**
- Eclipse Higgins: **www.eclipse.org/higgins/** & **http://spwiki.editme.com/HigginsInTheNews**
- Bandit: **http://forgeftp.novell.com//bandit/Bandit_f.pdf** & **www.bandit-project.org**
- Yadis: **http://yadis.org** & **www.openidenabled.com**
- OpenID: **www.openid.net** & **www.openidenabled.com**
- Private Credentials: **www.credentica.com**
- Liberty Alliance Project: **www.projectliberty.org**

Identity Management Research

- EU Future of Identity in the Information Society (FIDIS): **www.fidis.net**
- EU Privacy and Identity Management for Europe (PRIME): **www.prime-project.eu**

Select Analyst and Media Information Sources

- Federal Financial Institutions Examination Council, Authentication in an Internet Banking Environment, October 2005: Guidance document at: **www.ffiec.gov/pdf/authentication_guidance.pdf**
- National Consumers League, A Call for Action: Report from the NCL Anti-Phishing Retreat, March 2006: Press Release at: **www.nclnet.org/news/2006/Phishing_Report_03162006.htm**
- Gartner Survey Shows Frequent Data Security Lapses and Increased Cyber Attacks Damage Consumer Trust in Online Commerce, June 2005 at **www.gartner.com/press_releases/asset_129754_11.html**

Privacy Guidelines for RFID Information Systems (RFID Privacy Guidelines)

June 2006

Introduction

This document is intended to serve as privacy "best practices" guidance for organizations when designing and operating Radio-Frequency Identification (RFID) information technologies and systems.

The Information and Privacy Commissioner of Ontario (IPC) has a mandate to educate the public and address privacy questions raised by new information technologies, with a view to encouraging effective solutions. Accordingly, the IPC has developed these Guidelines in partnership with industry and other stakeholders[1]. The Guidelines are not intended to supersede any applicable privacy law or regulation.

We recognize that RFID tags are becoming more prevalent in our everyday lives, and offer many benefits and conveniences, such as from security access cards to ignition immobilizers to highway toll systems and other electronic pass systems.

RFID tags deployed in the supply chain process pose little threat to privacy – they are not linked to any individual but rather, placed on crates, pallets and cases to track products. They act as a unique identifier that uses Radio Frequency Identification for the automatic identification of products in the supply chain. These tags contain standard information pertaining to the products and do not include any personal information.

In order to allow RFID technology to realise its potential for consumers, retailers and suppliers, it is vital that we address privacy concerns prompted by the current state of the technology, while establishing principles for dealing with its evolution and implementation. Accordingly, we encourage organizations to observe and adopt the Guidelines contained in this document whenever deploying RFID technology with consumer-facing implications.

As indicated in the Commissioner's accompanying DVD, the use of RFID tags in the supply chain management process is not the problem. The problem arises with their use at the consumer item-level. RFID tags, when linked to personally identifiable information, present the prospect of privacy-invasive practices relating to the tracking and surveillance of one's activities. The goal of these Guidelines is to alleviate the privacy-related concerns associated with such data linkages, while increasing the openness and transparency associated with RFID systems. The use of these Guidelines will ultimately facilitate the preservation of trusted business relationships with existing customers, and perhaps assist in attracting new ones.

Scope

These RFID Privacy Guidelines apply to any organization that operates an information system involving the use of RFID technology on consumer products involving or potentially linking to, personally identifiable information.

1 EPCglobal Canada has been collaborating with the IPC in the development of these Guidelines, and will be seeking Board approval by its member companies to signify EPCglobal Canada's endorsement of these Guidelines.

"Organization" refers broadly to associations, businesses, charitable organizations, clubs, government bodies, institutions, and professional practices. In most instances, these Guidelines will be especially relevant to retailers.

"Information system" refers to any combination of RFID tags, readers, databases and networks that serve to collect, transmit, process and store RFID and RFID-linked information.

"Personal information" refers to any recorded information about an identifiable individual. In addition to one's name, contact and biographical information, this could include information about individual preferences, transactional history, record of activities or travels, or any information derived from the above, such as a profile or score, and information about others that may be appended to an individual's file, such as about family, friends, colleagues, etc. In the context of item-level RFID tags, the linkage of any personally identifiable information with an RFID tag would render the linked data as personal information.

These Guidelines are based upon the 10 principles of the 1996 Canadian Standards Association (CSA) Privacy Code, which were formulated by a wide range of stakeholders, including business, industry and consumer groups. The principles of the CSA Privacy Code now serve as the basis for Canadian privacy laws and regulations across Canada. They are observed by Canadian organizations in their day-to-day policies and practices, and are widely recognized as being one of the strongest and clearest expressions of privacy "fair information practices."

The Guidelines and their application are informed by the following three overarching principles:

1 **Focus on RFID Information Systems, not Technologies:** The problem does not lie with RFID technologies themselves; it is the way in which they are deployed that raise privacy concerns. For this reason, we prefer to speak broadly of RFID *information systems.* These Guidelines should be applied to RFID information systems as a whole, understood in their broader contexts, rather than to any single technology component or function.

2 **Privacy and Security Must be Built in from the Outset – at the Design Stage:** Just as privacy concerns must be identified in a broad and systemic manner, so too must technological solutions be addressed systemically. A thorough privacy impact assessment is critical. Users of RFID technologies and information systems should address the privacy and security issues early in the design stages, with a particular emphasis on data minimization. This means that wherever possible, efforts should be made to minimize the identifiability, observability and linkability of RFID tags with personal information and other associated data.

3 **Maximal Individual Participation and Consent:** Use of RFID information systems should be open and transparent, and offer individuals as much opportunity as possible to participate and make informed decisions.

This document provides voluntary, consensus-based guidance that recognizes the great variety of uses and applications for RFID technologies and information systems. Because of this heterogeneity, a degree of flexibility in its interpretation and application may be necessary.

We encourage organizations to adopt and to adapt these Guidelines for use in their own policies, procedures and applications, according to their own specific circumstances and needs.

RFID Privacy Guidelines

1. Accountability

An organization is responsible for personal information under its control and should designate a person who will be accountable for the organization's compliance with the following principles, and the necessary training of all employees. Organizations should use contractual and other means to provide a comparable level of protection if the information is disclosed to third parties.

Organizations that typically have the most direct contact and primary relationship with the individual should bear the strongest responsibility for ensuring privacy and security, regardless of where the RFID-tagged items originate or end up in the product life cycle.

2. Identifying Purposes

Organizations should clearly identify and communicate to the individual the purposes for collecting, linking to, or allowing linkage to personal information, in a timely and effective manner. Those purposes should be specific and limited, and the organizations and persons collecting personal information should be able to explain them to the individual.

3. Consent

Organizations must seek individual consent prior to collecting, using, or disclosing personal information linked to an RFID tag. To be valid, consent must be based upon an informed understanding of the existence, type, locations, purposes and actions of the RFID technologies and information used by the organization. Individual privacy choices should be exercised in a timely, easy and effective way, without any coercion. Consumers should be able to remove, disable or deactivate item-level RFID tags, without penalty.

Automatic deactivation of RFID tags, at the point of sale, with the capability to reactivate, should be the ultimate goal. Consumers should be able to choose to re-activate them at a later date, re-purpose them, or otherwise exercise control over the manner in which the tags behave and interact with RFID readers.

4. Limiting Collection

Organizations should not collect or link an RFID tag to personally identifiable information indiscriminately or covertly, or through deception or misleading purposes. The in-

formation collected should be limited to the minimum needed to fulfil the stated purposes, with emphasis on minimizing the identifiability of any personal data linked to the tag, minimizing observability of RFID tags by unauthorized readers or persons, and minimizing the linkability of collected data to any personally identifiable information.

5. Limiting Use, Disclosure and Retention
Organizations must obtain additional individual consent to use, disclose or link to personal information for any new purposes. Personal information should only be retained to fulfil the stated purposes, and then securely destroyed. Retailers should incorporate the data minimization principles outlined above, into and throughout their RFID information systems.

6. Accuracy
Organizations should keep personal and related RFID-linked information as accurate, complete, and up-to-date as is needed for the stated purposes, especially when used to make decisions affecting the individual.

7. Safeguards
Organizations should protect personal information linked to RFID tags, appropriate to its sensitivity, against loss or theft, and against unauthorized interception, access, disclosure, copying, use, modification, or linkage. Organizations should make their employees aware of the importance of maintaining the confidentiality of personal information through appropriate training. Although physical, organizational and technological measures may all be necessary, technological safeguards should be given special emphasis.

8. Openness
Organizations should make readily available to individuals specific information about their policies and practices relating to the operation of RFID technologies and information systems, and to the management of personal information. This information should be made available in a form that is understandable to the individual.

9. Individual Access
Organizations should, upon request, inform the individual of the existence, use, linkage and disclosure of his or her personal information, provide reasonable access to that information, and the ability to challenge its accuracy and completeness, and have it amended as appropriate.

10. Challenging Compliance
Organizations should have procedures in place to allow an individual to file a complaint concerning compliance with any of the above principles, with the designated person accountable for the organization's compliance.

Privacy and the Open Networked Enterprise

June 2005

Foreword

This white paper represents a joint effort between the Information and Privacy Commissioner of Ontario (IPC) and the New Paradigm Learning Corporation (NPLC). In 2004, the NPLC launched the Information Technology and Competitive Advantage program to examine the impact of information technology on **business** strategies in the 21st Century. This in turn led to the conceptualization of the "Open Networked Enterprise," or the O.N.E. This paper is an analysis of information privacy and security issues relating to **both** companies and consumers.

A number of high profile privacy breaches have drawn to the attention of consumers how important it is to be aware of who is in possession of their information and how it is being used. Consumers are getting much smarter, no longer blindly accepting that companies need to know everything about them in order to "serve them better" or get better products. Many businesses are now beginning to encounter consumers who want to have a say in what information they will give out and who is permitted to use it. Privacy is no longer just a compliance issue – it has become a business issue. The successful companies of the future will be those who accept the present-day fact that, *"privacy is good for business,"* and ultimately leads to a competitive advantage.

Ann Cavoukian, Ph.D.
Commissioner
June, 2005

The Idea In Brief

- Companies that take advantage of an Open Networked Enterprise (ONE) have the ability to become increasingly internet worked, and to share more and different kinds of information than ever before. But while this network allows for greater transparency of information, it also raises the central issue of privacy. By necessity, within an ONE corporate boundaries blur: in order to facilitate effective collaboration, the ONE compiles highly granular data from disparate sources (i.e., multiple stakeholders) to create a more holistic business intelligence. However, as active ONEs become increasingly global, this information may come from jurisdictions with looser privacy laws than the home company and, problematically, may overlap with personal information.

- At stake in this march toward global transparency is the value of information itself especially personally identifiable information (PII). The lifeblood of the 21st century economy, information must increasingly be viewed as both an asset and a liability that requires responsible management practices. A company adopting an ONE model is confronted with fundamental questions relating to its treatment of information:

    1 With whom will it share its PII?

    2 How will it manage that data internally?

3 How should it involve customers in managing their own PII?

4 What personal data will and should it receive from others?

5 Where should it set the limits of PII collection by new technologies?

New information technologies inevitably affect levels of personal privacy. History has taught us that excesses and abuses of personal information tend to provoke backlashes in the form of counter-reactive behavior by consumers and legislative/ regulatory bodies. Most, if not all, of the privacy issues described in this paper are currently subjects of heightened public awareness and controversy, and it is public awareness and controversy that lead to regulation and legislation.

For these and many other good reasons, a company's ONE model is well advised to meet the highest standards of responsible information management. By treating personal information responsibly, companies can harness the capabilities of a new breed of consumers privacy hawks who have strong views about personal information and privacy. Smart firms will build appropriate and effective privacy policies and practices into their systems. In doing so, these firms can avoid potential disasters and create the conditions for trust, loyalty, long-term relationships and economic advantage. Privacy is no longer a compliance issue; it is a business issue. It must be a business imperative.

The context: privacy and technology

Effectively capture, store and disseminate information on a mass scale never before contemplated. With the development of the photograph, telegraph and mass printing methods the world began to shrink. The emergence of the "yellow press" in the early part of the 20th century triggered the earliest definition of privacy as personal freedom from unwanted intrusions, or "the right to be let alone." From constitutional protection against search and seizure to restrictions upon free speech, to the implementation of slander and tort laws, common law in the 20th century tended to recognize and respond to privacy threats principally in terms of intrusion upon an individual's personal space and private conversations, as well as upon his or her good name and reputation.

The appearance of mainframe computers, centralized electronic databases and computerized records in the 1960s and 1970s triggered the next wave of privacy protections. The large scale collection by governments of secret, centralized dossiers on citizens and the frequent misuse of that information led to the development of laws to restrict governments' abilities to compile and use such records. At the same time, however, freedom of information laws were also enacted to promote greater openness and transparency, the sharing of new classes of information with multiple stake holders and to enhance individuals' rights of access to personal information in those databases.

In response to the misuse of large scale computerized databases by private organizations in the financial, credit and medical sectors, similar "sunshine" laws were also put in place to protect individuals and their highly personal information, such as credit or

health records. Fundamental "privacy" principles came into widespread currency, such as those set out by the U.S. Family Educational Rights and Privacy Act of 1974:[1]

- **Collection Limitation:** There must be no personal data record keeping systems whose very existence is secret.
- **Disclosure:** There must be a way for an individual to find out what information about himself or herself is in a record, and how it is used.
- **Secondary Usage:** There must be a way for an individual to prevent information about himself or herself, that was obtained for one purpose, from being used or made available for other purposes without consent.
- **Record Correction:** There must be a way for an individual to correct or amend a record of identifiable information about himself or herself.
- **Security:** Any organization creating, maintaining, using or disseminating records of identifiable personal data must assure the reliability of the data for their intended use and must take precautions to prevent misuse of the data.

By the late 1970s, information and communication technologies were facilitating a growing global trade in, and processing of, personal data. As various countries passed laws restricting the unlawful storage of personal data, the storage of inaccurate personal data, or the abuse or unauthorized disclosure of such data, worries arose that global trade would be constrained by the growing patchwork of national laws. In a far-sighted initiative, members of the Organization for Economic Co-operation and Development (OECD) came together and agreed to codify a set of principles that might serve as a framework for countries to use when drafting and implementing their own laws. The result was the 1980 OECD *Guidelines on the Protection of Privacy and Transborder Flows of Personal Data*, a document which expressed and described eight "fair information practices" as follows:

- **Collection Limitation Principle:** There should be limits to the collection of personal data and any such data should be obtained by lawful and fair means and, where appropriate, with the knowledge or consent of the data subject.
- **Data Quality Principle:** Personal data should be relevant to the purposes for which they are to be used and, to the extent necessary for those purposes, should be accurate, complete and current.
- **Purpose Specification Principle:** The purposes for which personal data are collected should be specified no later than at the time of data collection, and the subsequent use limited to the fulfillment of those purposes or such others as are not incompatible with those purposes, and as are specified on each occasion of change of purpose.

1 Family Educational Rights and Privacy Act (FERPA), (20 U.S.C. § 1232g; 34 CFR Part 99), 1974.

- **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
  - » with the consent of the data subject, or
  - » by the authority of law.
- **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.
- **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 stored personal data, and the main purposes of their use, as well as the identity and usual residence of the data controller.
- **Individual Participation Principle:** An individual should have the right
  - a) to obtain from a data controller or equivalent confirmation of whether or not the data controller has data relating to him or her;
  - b) to have communicated to the individual, data relating to him or her within a reasonable time; at a charge, if any, that is not excessive; in a reasonable manner; and in a form that is readily intelligible to the individual;
  - c) to be given reasons if a request made under subparagraph (a) or (b) is denied, and to be able to challenge such denial; and
  - d) to challenge data relating to him or her and, if the challenge is successful, to have the data erased, rectified, completed or amended.
- **Accountability Principle:** A data controller should be accountable for complying with measures which give effect to the principles stated above.

Since 1980, these voluntary "fair information practices" (FIPs) have been widely adopted around the world in statutes, standards, codes of practice, information technologies, and in norms and common practices. In Canada, for example, businesses, consumers and the government agreed to adopt a comprehensive set of privacy practices, known as the Model Code for the Protection of Personal Information (CAN/CSA-Q830-96), which was subsequently incorporated in its entirety into Canada's private sector privacy law. In the U.S., since the early 1970s, each successive government has remained committed to monitoring the "information practices" of organizations or, more specifically, the methods in which these organizations collect and use personal information and the safeguards they employ to ensure those practices are fair and provide adequate privacy protection. The result of this government intervention has been a series of guidelines and model codes that now represent commonly accepted principles, more formally known as Fair

Information Practices (FIPs). Common throughout the U.S., FIPs are five core tenets of privacy protection that have proven both successful and enduring:

- Notice/Awareness;
- Choice/Consent;
- Access/Participation;
- Integrity/Security;
- Enforcement/Redress.

The most essential principle of the five is the first: Notice/Awareness. Consumers need to have knowledge of an organization's privacy and information policies before any personal information can be collected and stored by that organization. This Practice specifically protects consumers: without such proper notice, they cannot make any reasonably informed decision regarding the use and disclosure of their personal information. Furthermore, the other principles are only relevant when the consumer has knowledge of an organization's information and privacy policies, and his or her rights as a consumer with respect to those policies. But despite this harmonization, significant variations persist in American law: the OECD Guidelines provide a floor, not a ceiling, for privacy protection.

Regardless of specific interpretation or manner of implementation, the OECD Guidelines and other similar FIPs accomplish two functions:

- They establish and confer broad rights on *individuals*, or data subjects, with respect to the collection, use and disclosure of their personal information by other parties.
- They set out broad responsibilities and obligations of *organizations* in respect to the collection, use and disclosure of personal information held in their custody.

The first function is commonly known as *information privacy*: the right or ability of individuals to exercise a measure of control over the collection, use and disclosure of their personal information by others. The second is *data protection*: the responsibility of organizations that collect, use, and disclose personal information to abide by an externally established set of rules.

It is important to understand the distinction between the two functions. The first approaches privacy from the perspective of the individual data subject, the second from the perspective of the custodial organization. Good privacy laws and data protection seek to reconcile the interests and objectives of both parties, but new technologies typically upset pre-existing balances.

What is personal information? Many organizations mistakenly believe that personal information is limited to basic "tombstone" data provided directly by the individual such as name, address, phone number, socio-economic details and so forth. Although statutory definitions vary around the world, personal information can include far more than this, such as:

- Any information associated or linked to an identifiable individual (e.g., personal preferences, beliefs, opinions, habits, family and friends)
- Physical and biological attributes (photo images, genetic data)
- Account numbers and any unique identifiers associated with an individual
- Transaction data (record of sales, customer service requests, returns, logins, phone calls)
- Transaction data of devices registered to an individual (phone numbers, computer logins, location data)
- Information about an individual provided by third parties (credit reports, employment references)
- Information inferred, derived, or generated from data held about an individual (profiles, scores)

Privacy and the ONE

Corporate Boundaries, Processes: How can privacy be protected in a business web? Will the ONE's modular, flexible approach to operations obscure or diminish accountability for unauthorized uses of customer data?

Modus Operandi: When employees become empowered to make decisions and try innovative approaches, will the devolution of authority diminish or enhance overall responsibility for, and adherence to, organizational policies intended to respect customer privacy? Conversely, will heavy handed workplace surveillance measures and practices discourage employee initiative?

Relationships: Will the ONE go beyond traditional top down approaches to engage and collaborate actively with clients, fostering what we describe as customer managed relationships?

Information Liquidity: How will the ONE manage the privacy risks associated with reliance on externally networked personal information and automated decision making?

Technology: Will the ONE steer clear of temptations to use new technologies to collect excessive personal information from customers and employees?

1.0 New Boundaries, New Business Processes

1.1 Context

As companies become internetworked, they share new kinds of information. Given that the ONE is increasingly global, as networks expand across national, as well as, statistical boundaries, the risks associated with information sharing increase: information may be shared between companies with different laws governing their treatment of and

responsibility to consumer privacy. In addition, ONE business processes are necessarily characterized by dense interconnections and constantly evolving relationships with a variety of internal and external partners, agents, affiliates and contractors. This modular approach to business affords high degrees of flexibility and adaptation to changing business environments and strategies. It also demands that the ONE focus on its core strengths.

1.2 Privacy concerns: outsourcing and offshoring

Personal data are increasingly handled by third party participants in information networks, and they are dealt with through outsourcing or offshoring practices. In general, "outsourcing" occurs when a company contracts out work to another company. "Offshoring" involves moving the work to another country, whether to a captive entity (i.e., a firm subsidiary) or to a third party supplier.[2]

Such third party data relationships are everywhere now, few businesses can survive without relying on other firms to help provide, process, or manage data. Whether exchanging data with business partners or sharing information internally, each transaction between businesses establishes a data relationship. These relationships must be carefully managed to ensure compliance with both an organization's policies and applicable external regulations around data protection.

In a b-web, information security is only as effective as the weakest link: "If one trading partner has a poor identity management program, another never tests its disaster recovery plan, and a third does not regularly assess its information technology outsourcers' compliance with information security policies, one's own security posture cannot logically rise above the lowest point achieved by these other entities."[3] As more organizations collaborate intimately, it becomes increasingly difficult for senior management to fully identify and manage the larger organization's ever growing risk interdependency. Collaboration has changed the security landscape; the behavior of a single organization can have a wide ranging impact on other b-web participants. Senior managers may think their organization is adequately protected when in reality their investments are undermined by process flaws. The statistic of such potential breaches is cause for concern: according to an Ernst & Young global survey, 80% of respondents failed to conduct a regular assessment of their IT outsourcer's compliance with the host organization's information security and privacy regulatory requirements.[4]

Reported information security breaches are occurring with increasing frequency, severity and cost to businesses.[5] Organizations are understandably reluctant to report data

2 Offshore Operations: Industry Feedback, Financial Services Authority (FSA), April 2005.

3 Global Information Security Survey 2004, Ernst & Young, p. 3 <http://www.ey.com/global/download.nsf/International/2004_Global_Information_Security_Survey/$file/2004_Global_Information_Security_Survey_2004.pdf>.

4 Ibid, p. 21.

5 See, for example, CSI/FBI Computer Crime and Security Survey (2002, 2004) <http://www.gocsi.com> and Ernst & Young Global Information Security Survey (2004) <http://www.ey.com/global/download.nsf/International/2004_Global_Information_Security_Survey/$file/2004_Global_Information_Security_Survey_2004.pdf> and Deloitte Global Financial Services Industry Outlook (2004, 2005) <http://www.deloitte.com/gfsi>.

security incidents, for fear of the negative effects on their competitive stance, public image and stock value. This reluctance is being trumped now by new accountability laws and regulations containing mandatory reporting requirements. Quite often, firms are not even aware that data security breaches have taken place if they occurred among business partners and affiliates. New data governance and similar compliance rules will strip firms of any reluctance to assume greater responsibility for and control over the actions of others.

The risks of outsourcing are thus known to be significant: it takes only one incident to damage years of brand building, and with the corporate identity go the trust, loyalty and business of customers, regardless of who is technically or legally liable. One cautionary tale of the risks of insufficient privacy monitoring involves a large national bank that outsourced its customer care and call center operations to a vendor in the Ukraine.[6] The company concluded contracts with the vendor to ensure that it took full responsibility for complying with all U.S. regulatory requirements, as well as with the bank's own privacy policy, which included a strict do not share with third parties for secondary uses without consent clause. The Ukrainian vendor also contracted to comply with strict data protection and information security requirements as per the U.S. Federal Trade Commission's Safeguards Rule. Nine months after operations began, thousands of U.S. customers began receiving charges on their credit card statements for magazine subscriptions and online services that they had never purchased. Hundreds complained that they became victims of identity theft, apparently a result of information leaks. A few customers reported that their entire bank balances had been transferred to untraceable locations. In response, the bank hired a forensic expert to determine where the possible data leak could have occurred. It was eventually discovered that the leak had transpired at an offshore outsourced location. It was traced to a new employee of the Ukrainian vendor who had remote access to the company's data warehouse. Notably, investigators found that the vendor's IT director had known about the leak months before the incident occurred, but never bothered to report it.

Such risks are not limited to offshore operations; companies should also determine whether domestic partners observe adequate security standards. In March 2005, for instance, the Federal Trade Commission settled a case in which a company that sold a shopping cart application to a web merchant then provided customer information to other entities, contrary to the merchant's privacy policy.[7] The web company had failed to ensure partner compliance before signing the contract.

The challenges to ensuring that security standards are met and maintained are significant. The average *Fortune 500* company typically has over 10,000 contracts and agreements with partners, affiliates, contractors and other third parties, all of whom

6 Dr. Larry Ponemon, "Are You Practicing Safe Outsourcing?," Darwinmag.com, April 2004 <http://www.darwinmag.com/read/040104/ponemon.html>.

7 "Internet Service Provider Settles FTC Privacy Charges," Federal Trade Commission, March 10, 2005 <http://www.ftc.gov/opa/2005/03/cartmanager.htm>.

affect the treatment of personal information. Just understanding data assets, uses and flows can thus be a daunting task, let alone subjecting these assets, uses and flows to clear and comprehensive policies, and enforceable procedures.

At the heart of the debate over privacy is the issue of corporate *accountability*. Organizations that are most visible or proximate to affected individuals bear most of the negative publicity and criticism for privacy breaches. When a privacy breach occurs, it will matter little to the public that the breach actually occurred at a partner's e-commerce payments processing website platform located in another jurisdiction; the organization that the customer deals with directly bears the most accountability and risk. As the most visible target, such an organization can suffer from diminution of brand and loss of credibility and sales, or by incurring the high costs of litigation, compensating victims, re-engineering information systems, or submitting to extensive audit and certification processes. When it comes to allocating blame, public perception can override corporate reality, and therefore the proximate organization must have the strongest incentive to ensure that personal information is managed responsibly.

1.3 Recommendations

Offshoring, outsourcing and third-party data relationships pose significant challenges to the governance of personal information. Meeting these challenges requires coordinated and ongoing management of multiple elements of data policy compliance and risk management across all entities in the data-sharing relationship. These elements include risk assessment, monitoring of the sharing relationship and prospective third parties, and substantial monitoring, tracking, classifying and regulation of enterprise data flows. But there is no "one size fits all" solution; the data collection, storage, use, sharing, oversight and enforcement needs of every firm are unique. We do know, however, that a comprehensive approach is more likely to be a successful one that accounts for people, processes, systems and policies.

Any solution must begin with a regulatory review: numerous laws, both current and proposed, restrict or impose conditions on offshoring and outsourcing activities. According to Alan Westin, founder of Privacy and American Business, provisions for protecting personally identifiable information will play a major role in anti-offshoring bills at federal and state levels. A significant data breach or identity theft scandal in just one overseas location could jump-start legislative responses. Ignorance of the law including potential laws will be no defense.

Legal requirements regarding the treatment or sharing of personal data will determine the ways in which risk is assessed, and the choice of assessment instruments and approaches. Europe, for example, prohibits transborder personal data flows unless certain "adequacy" requirements are satisfied. In the U.S., firms that outsource are already governed by numerous laws and regulations that impose compliance requirements, such as the *Sarbanes-Oxley Act*, the *Health Insurance Portability and Accountability Act* (HIPAA), the *Gramm-Leach-Bliley Act*, and the *Fair Credit Reporting Act*.

Outsourcing that involves personal data in particular has recently been drawing attention from regulatory bodies and the general public. Some state laws require that companies choose domestic over foreign workers to process employee data, while other states require disclosure if work on government contracts is undertaken outside the U.S. Maryland and Massachusetts vetoed similar bills in 2004, but it is expected that those bills will return. There are currently 115 anti-offshoring bills pending in 40 states; the majority aim to limit work contracted out by the state. Many aim also to prohibit state aid for overseas outsourcing, enforce disclosure of call center locations, restrict outsourcing of personal sensitive data such as health or financial, and in some cases to require consent from customers.

California's legislature passed five anti-offshoring bills in 2004. Protective measures included allowing no state contracts for work performed outside the U.S. and no outsourcing of Social Security Numbers, drivers' licenses and personal health data. One particular law required overseas call centers to disclose their location to residents of California and local employers to report to the state if they moved operations offshore. Governor Schwarzenegger ultimately vetoed all five bills, but the backlash was significant; it is likely that these bills will re-emerge for a second attempt.

Regulations exist at the national level as well: the U.S. Senate passed the Dodd Bill in 2004, which prohibits the awarding of federal contracts to companies with overseas employees. A proposed House resolution also seeks to enforce consent prior to transferring sensitive personal data to countries that lack adequate privacy protections as defined by the Federal Trade Commission. Hillary Clinton's proposed "Safe ID Act" will prohibit businesses from processing sensitive personal information in foreign countries without offering an opt-out choice to the public. In addition, if the Act passes, businesses will become directly liable for any privacy breaches.

In such an environment, rules for data flows and uses should comply across all jurisdictions to established international benchmarks, like COBIT[8] and ISO 17799.[9] Adherence should be monitored through due diligence, site visits, contractual remedies and third party audit and certification.

To manage an ONE effectively a company must develop a comprehensive set of objectives and policies regarding privacy and security of data uses and flows. These policies must be clearly expressed and effectively communicated throughout the ONE and to all third parties. Some elements to consider:

- Minimize data collection, use and security among partners
- Develop strong contractual agreements and deterrents for third parties
- Deploy continuous monitoring, auditing and enforcement mechanisms

8 Information Systems Audit and Control Association, <http://www.isaca.org>.

9 ISO 17799 Directory, 2005 <http://www.iso-17799.com>.

- Implement privacy crisis management protocol in the event of a breach
- Develop adequate consumer trust to draw upon in the event of an incident (customers may be more forgiving)

Information and communications technologies (ICTs) can also help maintain security for consumers: firewalls and other filtering software, secure transmissions, handling and storage of data, strong authentication, access controls, extensive logging and audit trails, and other safeguards can be assured in part through ICTs, and can significantly increase consumer security. It must be remembered, however, that a critical element of success fully deploying such systems involves comprehensive education, training and awareness programs for all employees involved in these processes.

With regard to *transparency*, current U.S. legislation requires firms to disclose their outsourcing policies and practices to customers. Knowing that customers will be informed about outsourcing arrangements might motivate companies to make sure those arrangements are secure. One U.S. financial company, E-Loan, not only explains its outsourcing practices to its customers, but actually offers them a choice of whether they would like their financial arrangements processed in-house.

2.0 Modus Operandi

2.1 Context

The modus operandi of the ONE is characterized by flatter hierarchies, greater collaboration, devolved decision making, more risk taking, high flexibility, agility, adaptability, and innovation.

2.2 Privacy concerns: the insider conundrum vs. internal surveillance

In such collaborative environments, organization-wide privacy and security policies governing the use of data can be difficult to implement and enforce. Because such policies are often mandated from above, their hierarchical quality may conflict with the more open, collaborative culture of the ONE. Often such policies are perceived as barriers to new and innovative thinking, products and practices.

At the same time, flatter, decentralized organizations may be well connected, but they are also more vulnerable. The more that senior management has lost its situational awareness *(the degree of accuracy by which perception of the current environment mirrors reality)* the less likely it will be able to comprehend the organization's ever growing interdependence. Single events can have profound impacts that cascade across the network. Furthermore, when individual employees are empowered, how do you ensure that they respect privacy policies and principles? How do you ensure that data is protected? If *everyone* is responsible for privacy and security, then perhaps *no one* is.

Recent data privacy and security breaches have focused the public and lawmakers' attention on the poor information management practices and procedures of businesses, especially since large-scale losses and theft of personal information can have profoundly negative effects on innocent individuals.

2.3 The insider conundrum

It is not uncommon for marketing and communications departments, in the pursuit of quarterly objectives and hard metrics (and when given a free hand), to develop initiatives that bypass privacy policies. In their efforts to ensure security, IT departments want to control and lock down all information assets, often by filtering and logging everything, or otherwise engaging in what could be perceived as nosey employee surveillance practices. Software development teams may add invasive privacy and security features to products that act as spyware. Overzealous human resources departments, looking for the perfect employee, may carry out deeper background checks than necessary or engage in psychological profiling. Any of these activities can land a company in hot water.

Sometimes personal data exposure or misuse occurs by accident, such as when pharmaceutical giant Eli Lilly accidentally exposed the email addresses of 669 Prozac users in the "To:" field of an email marketing solicitation, resulting in an FTC investigation and settlement, as well as a tarnished brand and reputation.[10] Quite often, such data loss or unauthorized exposure occurs as a result of negligence or failure to follow simple policies and procedures, such as when laptops with unencrypted personal data go missing, or when default passwords are not changed.

Inside theft is a big problem. It is well known that insiders who access databases often have network authorization, knowledge of data access codes and a precise idea of the information they want to exploit. Surprisingly, most database applications even sophisticated high-end ones store information in "clear text" that is completely unprotected.

Further, there are more unauthorized accesses to databases than corporations admit to their clients, stockholders and business partners, or report to law enforcement. Gartner estimates that internal employees commit 70% of information intrusions, and more than 95% of the intrusions result in significant financial losses. A 2002 survey of 163 *Fortune 1,000* companies found that 70% of reported security breaches were linked to insiders.[11]

Another survey by the Computer Security Institute revealed that over half of all corporate databases have some kind of breach every year, and the average breach results in close to $4 million in losses.[12] And these are just the security problems that companies report!

10 "Even the unintentional release of sensitive medical information is a serious breach of consumers' trust," said the Director of the FTC's Bureau of Consumer Protection. "Companies that obtain sensitive information in exchange for a promise to keep it confidential must take appropriate steps to ensure the security of that information." <http://www.ftc.gov/opa/2002/01/elililly.htm>.

11 Richard Mogul, "Danger Within—Protecting your Company from Internal Security Attacks," *CSO Online*, August 21, 2002 <http://www.csoonline.com/analyst/report400.html>.

12 Computer Security Institute/FBI Computer Crime and Security Survey, 2002.

Non-technical and behavioral forms of intrusion are also common. What makes the insider threat so daunting is that most breaches do not require sophisticated methods, and they most often occur on-site during normal working hours by employees, freelance contractors, employees of corporate contractors, and even clients. In some cases, disgruntled employees simply wish to hurt an organization and its reputation.

Finally, there are the security problems associated with external hackers, thieves, and con artists. Why steal one identity from a trash bin when you can steal a million from an insecure database?

Consider some recent breaches:

- Time Warner reported that a cooler-sized container of computer tapes containing personal information of 600,000 current and former employees was lost on its way to a data storage facility in March 2005. The computer tapes contained the names, SSNs, and other data pertaining to current and former employees dating back to 1986.
- Data broker ChoicePoint reported the unauthorized access of over 150,000 detailed dossiers by scam artists over a period of a year. At least 700 known instances of identity theft resulted from this security breach. Poor access control and authentication procedures were blamed.
- Online brokerage Ameritrade disclosed in April 2005 that it had lost a backup computer tape containing records of 200,000 customers.
- A former employee of a Washington area Blockbuster Video store was indicted on charges of stealing customer identities and using them to buy more than $117,000 in trips, electronics, and other goods, including a Mercedes-Benz.
- LexisNexis reported a privacy breach in its Seisint database division. Hackers accessed more than 300,000 profiles, including SSNs and driver's licence numbers more than 10 times the number originally reported. The company blamed poor access management practices.
- A California medical group is currently informing nearly 185,000 current and former patients that their financial and medical records may have been compromised following the theft of computers containing personal data.
- Healthcare giant Kaiser Permanente notified 140 patients that a disgruntled former employee had posted confidential information about them on her blog.
- Tokyo Disney amusement parks reported that personal information on 122,000 customers who bought one-year admission passes in 2002 was leaked. Several hundred received fraudulent phone calls or direct mail.
- Bank of America admitted it lost backup tapes containing personal information on 1.2 million federal employees, including several Congress members.

This string of high profile data security breaches has sparked a public firestorm and closer lawmaker scrutiny of businesses' information management and security practices. A flurry of proposals at federal and state levels intends to ensure that businesses assume more responsibility and liability as custodians of personal data.

In response, businesses have invested heavily in information security. A significant and growing percentage of corporations routinely monitor employee behavior and activities such as web surfing and email use. We are seeing a strong surge in interest and demand for identity management, authentication, and role based access systems that track and monitor virtually every employee activity.

The concept behind these security efforts is clear: information is an asset, and access needs to be controlled and predicated on strong identification, authorization and auditability.

Strong security enhances privacy, but this trend seems counter to ONE culture. We are seeing a rise in employee litigation against companies in reaction to excessive monitoring and surveillance. Employee privacy is being pitted against customer privacy and employees are losing.

The fundamental problem, again, is ensuring accountability and governance of personal data while respecting the privacy of customers, data subjects and employees. The rogue actions of some empowered staff, however well-intentioned, can have negative effects on the entire organization. At the same time, a heavily monitored and restricted workforce can become less empowered and more resentful, ultimately to the detriment of the ONE.

2.4 Possible solutions

As with any information privacy and security program, there is no "one size fits all" solution. Every organization is unique, and a lot depends on the nature of the business, the personal information at stake, and the degree of vulnerability and risks involved.

A continuous privacy awareness and training program for employees is a requirement for success. In fact, the most successful ONEs have well developed corporate cultures of customer privacy *and* respect for employees. Clear and comprehensive privacy policies, effectively communicated and enforced, ensure that privacy and security are infused throughout the organization and promoted as everybody's responsibility. It is also not uncommon for performance appraisals and bonuses to be tied to adherence to corporate privacy policies. At the same time, clear and consistent policies on employee surveillance, communicated well and carried out in a fair and impartial manner with appropriate curbs on potential abuses can go a long way in dissipating employee fears, resentment, and counterproductive behavior.

Privacy and security leadership is also a necessity: firms require a strong chief privacy officer (CPO) who understands all aspects of the organization and is capable of navigating and working with all departments. When vested with appropriate oversight

and/or veto authority, such an individual can become a champion for privacy within an organization, be able to bridge the divides between higher and lower management and between different corporate divisions, and become the "go to" person whenever there are questions or incipient problems. A champion for strong data privacy and security, the CPO can also put in place credible and effective policies governing the use of workplace monitoring technologies without raising employees' concerns about excessive surveillance. A good CPO can reconcile the apparent contradictions between strong data security and employee privacy on the one hand, and the operational needs of the ONE on the other, thereby fostering a climate of trust and collaboration.

Perhaps most significantly, and today more than ever before, the CPO uses new technological tools and automated mechanisms. For example, new database and data flow "discovery tools" can map organizational information flows and minimize security risks by automatically detecting and responding to possible data misuses at the earliest possible stages through heuristic intrusion detection systems. Similar tools exist to evaluate website compliance to privacy and security standards. There has also been a growth in interest in enterprise identity management, access control and automated content filtering systems.

Just as inbound electronic communications can be scanned for viruses and inappropriate content, so too can outbound messages be scanned for protected intellectual property and "leakage" of sensitive personal information. Best of all, these tools can be automated so that "surveillance" need not be arbitrary or performed by a human, except when suspicious incidents are flagged for follow-up.

The emergence and growth of data security technologies and systems has been remarkable. Such technologies are far too numerous to mention here, but a knowledgeable CPO or Chief Information Officer, would be well aware of the latest data security systems.

Technological tools can also be effective in establishing audit trails. One promising solution is to attach a "condition of use," such as client privacy preferences, directly to the data, so that privacy and security policies are effectively "bound up" with the data the client supplies. The rules relating to data use are "wrapped around" the data itself. In this way, many data privacy and security policies can be demonstrably self-enforcing, with little or no need for direct CPO intervention or oversight. IBM's Tivoli Privacy Manager is one such successful tool.[13]

2.5 Summary

As information needs continue to grow, so too will the challenges of complying with a widening range of anticipated regulatory privacy and security requirements and public expectations. A strong culture of privacy and security, and of employee respect and trust, is the foundation for a successful ONE. To maintain agility and flexibility, an empowered Chief Privacy Officer is needed to install the proper mix of policies,

13 <http://www-306.ibm.com/software/tivoli/products/privacy-mgr-e-bus>.

procedures, training and technologies that will serve both to manage personal data throughout the ONE's lifecycle *and* to assure employees that they are not being unfairly watched.

3.0 Relationships

3.1 Context

The success of a company's ONE is a function of positive experiences and strong relationships with customers. Word of mouth endorsements are among the most valuable types of marketing any organization can have, and by providing useful, efficient, personalized services and products, the best companies foster enduring trust, loyalty and repeat business. So valuable is the repeat value of a customer that, increasingly, products are given away at discounted prices in favor of establishing a long-term relationship.

3.2 Privacy concerns: consumer trust

In today's hyper-competitive climate, brand and reputation are shorthand vehicles for conveying trusted information, and fostering and reinforcing positive experiences with customers. Trust takes a long time to build, but a short time to erode and lose. Trust is built by making and keeping promises over time, and being transparent and reliable about your commitments and policies.

In order to build a more intimate relationship with consumers, businesses are adopting novel techniques to serve customers with personalized services, such as discounted loyalty cards. Integrated customer relationship management (CRM) technologies provide holistic views of customers, their data and their transaction histories, while providing customers with convenient single-window "no wrong door" portals for efficient service.

We are seeing a trend towards relationship and permission-based marketing in an effort to engage the customer in an ongoing, personalized, customized, 1:1 manner.[14] Such marketing techniques depend on collecting and collating as much information as possible about the client in an effort to differentiate, understand and respond to clients' specific needs and wishes *(ideally before they themselves recognize this!)*.

Permission-based marketing may result in less data than that obtained through arbitrary online registrations, but the information thus collected is, without a doubt, far more relevant. Further, permission-based marketing also builds loyalty through trust. To use an analogy, a lot more can be accomplished with a sniper's rifle than a shotgun. A case in point: a 2003 survey of over 1,000 persons across the United States found that 70% of respondents were willing to receive legitimate email marketing messages provided that they had given their consent.[15]

14 Seth Godin, *Permission Marketing* (New York: Simon & Schuster, 1999).

15 "Digital Impact Sponsored Survey Shows Majority of Internet Users Request Legitimate Email Marketing Messages Despite Increasing Concerns Over Spam," *Digital Impact*, December 8, 2003 <http://www.digitalimpact.com/ newspress120803.php>.

In the Spring of 2005, Ipsos-Reid conducted a survey that reported that the number of respondents willing to receive commercial email was increasing, again with the caveat that they had given their permission. The survey found that close to 80% of Internet users have registered to receive email from an average of nine commercial websites.[16] Combined with the latest email filters, Internet users can now customize their choice of exactly which companies are allowed into their inbox, and who goes directly to the trash file.

Thin Data, a Toronto based email service provider, began a permission based marketing campaign on behalf of Mirvish Productions, a theatre production company in Toronto, Canada. Thin Data sent a monthly email newsletter to over 15,000 subscribers and found it was read by 65% of recipients per month. In comparison, it found that less than 30% of recipients of indiscriminate direct mail campaigns opened emails.[17]

Permission-based marketing, suggests Seth Godin, is like dating.[18] The company or marketer approaches the consumer to request a date. If the consumer says yes, they go out, and if both parties are interested, self-disclosure of personal details takes place. Trust builds over time, and the relationship may continue, perhaps for years, and in some cases, a lifetime.

Building on the idea of permission-based marketing, the concept of the "Customer Managed Relationship" (or CMR instead of CRM) has emerged, where the customer manages the relationship with the company and controls his or her own data. The most popular industry view holds that customers should own their own personal profile and have access to all the information about themselves across all departments. Additionally, the CMR system should be designed around consumers' needs and desires. An example of this would be Vivendi Universal's Universal Music Mobile, launched in 2001 as one of the first CMR-oriented services offered. The Mobile provides an assortment of music-related multimedia services, and self-service, combined with the billing program, is a major feature of the service: it allows customers to activate multiple services and features online, view their usage, pay or pre-pay online, change service options online, modify their contract, or change billing details themselves. Vivendi Universal took a relatively early lead in letting its customers define how they wanted to communicate with the company, not the opposite. In this kind of relationship, consumers feel a sense of empowerment and control (which equals a feeling of trust and security) over their personal information. IBM Chief Privacy Officer Harriet Pearson refers to this kind of relationship as a "trusted balance" – a willingness to communicate and put into effect a concise set of privacy rules.[19] Also crucial is the fact that this arrangement is about selling an emotion or an experience, the same way that Nike sells an athletic lifestyle. The key to success in a CMR is thus allowing customers not only

16 "E-mail ad firms winning war against spam," *The Globe and Mail*, March 15, 2004, B11.

17 Ibid.

18 Seth Godin, *Permission Marketing* (New York: Simon & Schuster, 1999).

19 Aiden Barr, "Privacy is Good for Business," 306.ibm.com, 1999 <http://www-306.ibm.com/e-business/ondemand/us/customerloyalty/harriet_pearson_interview.shtml>.

to feel in control of their choices as consumers, but also to be able to monitor and manage their own personal information. If they participate in a CMR by choice, it is a sure sign they trust the company.

But despite growing privacy protocols, people are increasingly wary about disclosing unnecessary information about themselves. If customers think information requests are superfluous, intrusive or unnecessary, they may lie or abandon the process. "Relationships" that are not founded upon genuine dialogue, reciprocity and negotiation can flounder, such as when privacy promises are obscure and written in vague non-commitant legalese (and subject to change at any time). Even worse is when the defaults are invasive or perceived to be disrespectful of customers' wishes, such as when a website's registration default is "opt-in."

As far as youth are concerned, it would be an error to dismiss them as apathetic when it comes to concern over privacy. The 2004 Harris Interactive survey of youth found that many of them do, in fact, care. The degree of concern with "privacy being invaded online" varied by age, with the lowest being 8- to 9-year-olds at 25%, and the highest being 18- to 21-year-olds at over 50%.[20]

"Privacy hawks," as dubbed by Ben Charny, engage in "privacy self-defense" by employing guerilla tactics to protect their personal information.[21] The Pew Charitable Trust describes these cyber renegades as most likely male, with over a third between the ages of 18 to 29, who have been online for three or more years and make up 25% of the Internet population. While by no means a homogeneous group, they hold one common belief: their personal information will ultimately be exploited and "privacy policies" are not always to be trusted. Therefore, they feel that falsifying their personal information is necessary out of self-defense.

In terms of specific tactics to maintain personal privacy, the most common is to simply lie. Those who are aware of a website's limitations under-stand that they can, with impunity, provide completely false information on a registration form to qualify for access. For some it is even a game of sorts: one can declare oneself as a CEO who lives in Beverly Hills and makes between $0 and $15,000 per annum. Indeed, it would not be surprising to find that the most common zip code entered on website registration forms is 90210, from the popular 1990s television show, or that Bill Gates has registered with MSN more than one hundred times.

To date there has been only a handful of in-depth studies conducted on individuals who lie when registering online. In 2000 it was found that 20% to 30% of registrants lied (with teenagers being the highest scoring age demographic), but this is considered a conservative estimate.[22] The main reasons cited for lying included distrust over

20 Harris Interactive, *Youth Pulse*, June/July 2004, p. 64.

21 Ben Charny, "Protect your Internet privacy… by lying," ZDNET News, August 21, 2000 <http://news.zdnet.com/ 2100-9595_22-523232.html>.

22 The Pew Internet and American Life Project, "Trust and Privacy Online: Why Americans Want to Rewrite the Rules," August 2000 <http://www.pewinternet.org/PPF/r/19/ report_display.asp>

how personal information would be used, avoiding junk mail, and a desire to remain anonymous. This desire for continued privacy is something to take into account when considering the ROI of advertising and marketing budgets.

Another growing method of consumer self-defense is having a secondary, or "disposable," email address. Anyone can log onto Hotmail in five minutes and create an email account based entirely on false information. A 2004 Harris Interactive survey found that youth aged 10 to 21 had an average of two to three email addresses.[23] Some websites such as *Dodgeit, Mailinator, Spamgourmet* and *Spambob* now even offer free disposable email accounts. In the Spring of 2005, *Spamgourmet.com* reported that it had almost 90,000 subscribers with nearly 1.5 million disposable email addresses. The Pew Internet and American Life Project found that 20% of persons who use the Internet have used disposable email addresses, while the number of teenagers who did the same was as high as 56%. It should also be noted that disposable email addresses are not only used to avoid junk mail; they are also a safe vehicle for entering contests, or registering for free gifts or rebates (the address is disposed of once the contest is over, or the gift or rebate has been received).

Privacy hawks and anyone else who wants to remain anonymous online have received help from advances in Internet technology. Mozilla Firefox is an Internet browser that allows for anonymous surfing. Most browsers now include toolbars equipped with a function that blocks pop-up ads and cookies. And almost all email services now come with "block sender" and "junk mail" options that automatically vet email. There is also a host of commercial and free software programs available, such as Ad-Aware and BetaSpyware, that provide real time defense against unwanted intrusion from hackers and marketers, and other forms of surreptitious data gathering. In fact, these features are becoming so commonplace that disposable email addresses may soon be redundant, because even if unwanted contact is made, a simple click of a button can ban a marketer or advertiser indefinitely. As of April 2005, Ipsos-Reid reported that 77% of Canadians already use such filters while online.[24] In 2003, the Pew Internet and American Life Project found that 37% of Americans used filters while online.[25] In 2005, the number of families with teenagers in the U.S. that used online filters at home was found to be 54%, up from 41% in 2000.[26]

Self-defense of personal privacy is a growing movement, no longer limited to the actions of a few privacy hawks. People are becoming more and more organized; they are becoming connected in their common goal. Strategies, techniques, and tactics in defense of one's privacy are now becoming widespread topics of conversation in chat rooms and on blogs.

23 Harris Interactive, *Youth Pulse*, June/July 2004, p. 53.

24 Ipsos-Reid, "Canadians Winning the War Against Spam," *Ipsos*, March 10, 2005 <http://www.ipsos-na.com/news/pressrelease. cfm?id=2594>.

25 Pew Internet and American Life Project, *Spam Survey*, June 10-24, 2003, p. 20.

26 Pew Internet and American Life Project, *Protecting Teens Online*, March 17, 2005, p. 8.

Microsoft's small business website offers a top-ten list for successful permission based email marketing, with number ten being *always remember the network effect*. "Bad news travels much faster than good on the Internet. An angry online customer can broadcast his ire to millions by creating an 'I hate [your company]' website, emailing an account of their experience to friends, posting it on message boards and other ways. Remember, in this economy the customer is in control."[27] For further reading on anti-company websites, Forbes.com has published an online article featuring the top corporate "hate" websites.[28]

3.3 Possible solutions

Strong, clear and overt privacy commitments, honored over time, demonstrate respect for the customer and foster trust and loyalty.

Customer knowledge and consent should be prerequisites for all marketing activities. The customer should be given every opportunity to become a participant in the marketing process, and to provide feedback and direction. New technologies make it possible for organizations to give their customers direct access to all data held on them, as well as other self-serve options.

Trust and brand are easily eroded when privacy commitments are not perceived to be honored, or when the client is denied meaningful opportunities to be a participant in the "relationship." Let CRM morph into CMR!

When it comes to personal information, not sharing is caring. Your customers will thank you. Successful companies need to take a long-term strategic view of value of their customer data and resist the temptation to share it or sell it to third parties without their customers' consent.

Conversely, people will not lie when they feel there is a trusted connection between themselves and a company. They will almost invariably give their personal details if they think a relationship with a particular company is going to benefit them, even if all they want is to stay informed of the latest trends on products and services of interest. And isn't that precisely what you want to pitch to them? Find out what your customers want and give it to them they will keep coming back for more. But give them what they **do not** want and you will drive them away. You decide.

Your privacy mantra should be, "Always ask, never assume."

4.0 Information Liquidity

4.1 Context

An ONE aggregates data from disparate third-party sources to create business intelligence that, in turn, may overlap with personal information. Many public databases contain private information that firms can easily access. How can privacy be protected?

27 Derek Scruggs, "10 rules for successful permission-based e-mail marketing," Microsoft.com/small business, April, 2005.

28 Charles Wolrich, "Top Corporate Hate Web Sites," Forbes.com, March 8, 2005.

4.2 Privacy concerns: bad data, bad decisions

"Search, don't sort" is Google's motto and advice to customers. This advice is particularly apt at a time when technology provides individuals and firms with the ability to instantly find, aggregate and distill a virtually unlimited quantity of information for novel uses and competitive purposes.

Taking advantage of this new wealth of data, a new and rapidly growing industry has arisen to collect, analyze, and sell aggregated personal information and profiles. The types of companies that do this are varied, such as TransUnion and Experian, which are credit bureaus to LexisNexis, and most notably ChoicePoint, which is described as a data miner and aggregator. By far, ChoicePoint is the largest data aggregator on the market, with billions of public records in its database.[29] With data that includes motor vehicle registrations, license and deed transfers, military records, names, addresses and SSNs, ChoicePoint routinely sells dossiers to police, lawyers, reporters, private investigators and even to the U.S. Department of Homeland Security.

The direct marketing industry has been transformed and spurred on to new heights by the online environment, where all manner of technologies are being deployed to collect highly granular personal information that is then combined with data available elsewhere and used to profile and predict behavior. Examples of these technologies include use of "cookies," "web bugs," and other electronic tools and agents that track online activities.

Attempts to consolidate information is not always successful, however. For instance, online advertising giant DoubleClick's attempt in 1999 to purchase Abacus Direct for $1 billion in order to merge data on Net surfing habits from the 5 billion ads DoubleClick served per week and the 2 billion personally identifiable consumer catalog transactions recorded by Abacus was vigorously opposed by privacy advocates and consumers on privacy grounds, prompting a three-year investigation by the FTC. The deal ultimately failed.

Personal consumer information is incredibly valuable to corporations. When Air Canada fell into bankruptcy proceedings, the airline sold off its information assets, which consisted of millions of profiles of Aeroplan members from its popular loyalty program, for nearly CDN$1 billion about three times the market capitalization of the company's airline fleet.

So lucrative is the information profiling industry that online marketers have formed numerous lobby groups and associations such as Network Advertising Initiative (NAI) and Online Privacy Alliance (OPA) in order to help shape the evolution of new laws and regulations that could have a direct impact on their business models.

The marketplace for personal information is estimated to be in the tens of billions of dollars per year in the U.S. alone, with businesses as the main customers. In the past six months, several new books documenting the extent of the information aggregation and

29 Bob Sullivan, "Database giant gives access to fake firms," MSNBC, February 14, 2005 <http://msnbc.msn.com/id/6969799>.

profiling industry have hit the market. Among the best are *The Digital Person: Technology and Privacy in the Digital Age*,[30] by Daniel Solove, and *No Place to Hide*, by Robert O'Harrow, Jr.[31]

Personal information is collected and sold to firms for a fast growing variety of purposes. Detailed dossiers on individuals are bought and sold like any commodity in a vast and growing "grey market" in order to carry out background checks, to authenticate people, credentials, and claims, to evaluate individual risk, to generate client profiles and make behavior predictions, to establish metrics, for billing purposes, and for a wide range of "research" purposes, such as marketing and national security. Such information is routinely used by business to make decisions affecting individuals, such as whether or not to hire or promote them, or to grant them credit or insurance, and in general to establish the terms of a company's relationship with an individual.

The availability and use of detailed dossiers on individuals, and the derived profiles or scores, is seen as beneficial to individuals and to society because it helps detect and deter fraud (e.g., in the form of employment background checks); it helps lower transactions costs (e.g., the "miracle of instant credit"); and it enables better servicing of customer needs (e.g., by providing customer profiles). The general goal behind tapping huge database grids is to make more informed, smarter decisions.

Unfortunately, too much personal information liquidity and automated processing can be a liability. The history of privacy in the 20th century has shown that the abuse of personal information collection often provokes public outcries, backlashes, and new regulations and liabilities for organizations that act as data custodians especially when individuals are negatively affected as a result.

We may in fact be witnessing a "perfect privacy storm" right now in the wake of an endless series of large scale privacy and security breaches reported almost daily in the news. Given the ever increasing incidence of identity theft, the public and lawmakers are beginning to demand that businesses begin to shoulder their fair share of responsibility for the many negative effects and costs that fall upon innocent third parties as a result of data mismanagement. New federal laws and regulations are widely expected within the year that will curb excessive business practices involving personal information collection, use and disclosure, and to arm individuals with better knowledge and greater rights of access and redress vis-à-vis those businesses that would collect and use their personal information.

As noted earlier, the excesses of the yellow press in the early 20th century spawned the concept of the right to privacy, and led to a variety of legal restrictions and tort remedies for affected individuals. Similarly, abuses of centralized state dossiers and financial credit reports led to the waves of law, regulation, and litigation intended to curb the activity and provide various rights to individuals. Today, similar concerns about the ex-

30 Daniel J. Solove, *The Digital Person* (New York: New York University Press, 2004).

31 Robert O'Harrow Jr., *No Place To Hide*, New York, Simon & Schuster, 2005.

tent and accuracy of personal data contained in blacklists, especially those shared with and used by governments, are the subject of considerable public debate.

Moreover, high-profile stalking and murders (e.g., Rebecca Schaeffer, Amy Boyer) that were facilitated by access to sensitive personal information led to new restrictions and liabilities on the use and disclosure of sensitive personal information. A desire to protect children led to other controls on information about individuals under the age of thirteen. The negative effects and costs of spam, telemarketing and spyware are also provoking new controls. Most recently, the ChoicePoint data breach has focused the regulatory spotlight on the practices and liabilities of large "infomediaries" who collect and sell personal information. In February 2005, it was discovered by an internal employee of ChoicePoint that identity thieves, in a plot twist taken from a Hollywood movie, were creating false identities to establish accounts with ChoicePoint and then using those accounts to commit identity theft. The employee became suspicious when he noticed that applications from some businesses were coming from a nearby Kinko's. ChoicePoint reacted by notifying close to 200,000 persons, as required by California law, that their personal information may have been compromised. However, the Los Angeles police department believes that as many as 500,000 persons may have been affected.[32] As of April 2005, there are 39 bills (pending in 19 states)[33] that are modeled after California's *SB1386*, which is known for its clause requiring that persons be notified when their personal information has been breached.

There is growing sentiment among lawmakers to place more accountability and liability on those organizations that have used personal information in irresponsible ways. The FTC has shown a willingness to investigate firms that do not live up to their privacy promises and who otherwise engage in unfair and deceptive trade practices involving the use of personal information.

Common privacy issues and liabilities include the following:

- **Failing to inform or seek the permission of the customer to obtain personal information from other sources,** then collating with data provided directly by the customer.
- **Failing to get explicit informed consent from the customer** to share his or her personal information with third parties and other members of the intelligence network.
- **Obtaining and using old or inaccurate data obtained from third parties.** If incorrect data are used to make decisions affecting an individual, the ONE must be prepared to justify its decision-making and face the consequences when incorrect.

32 Our Georgia History, *ChoicePoint Scandal*, April 2005 <http://www.ourgeorgiahistory.com/chronpop/1000072>.

33 Emily Hackett, *The Problem of Data Security*, Internet Alliance, April 25, 2005.

- **Automated processing and decision-making can also lead to discriminatory treatment of customers, with no recourse for action.** For example, customers with "undesirable" phone numbers will wait long service times while "desirable" phone numbers get through to customer service right way. Who is accountable when customers are denied service because they have erroneously been placed on a secret networked blacklist?

Networked intelligence and automated decision-making tools can be of a great service to the public, but a very real danger exists in that incorrect or outdated personal data can propagate throughout these systems. Again, accountability and responsibility are often diluted when personal data, and in this case, incorrect assessments, are available everywhere, instantaneously.

Companies that rely on other sources for their information and decision-making needs must understand that they may nonetheless incur liability and penalties for failing to take responsibility for their actions.

4.3 Possible solutions

As the ONE increasingly taps into the grid of available personal data, it must ensure that this information is

- Legally acquired, used or shared
- Sufficiently accurate for the identified purposes
- Appropriate and proportional for those purposes
- Used in a transparent and defensible manner
- Available for access and correction by the individual

Organizations must be clear and up front about the nature and extent of their information activities involving third parties. For example, a considerable amount of sensitive personal information may be acquired from various sources in order to screen potential employees. The routine sharing and use of information among a large number of affiliates, partners, and subcontractors in the corporate "family" should be made explicit.

Firms should also always explain and justify the use of automated decision-making tools. Wherever possible, they should seek the informed consent of their customers, and be prepared to provide access and correction to all data about an individual (not just information supplied directly by the individual), along with an explanation of specific data items. If consent is withdrawn, then the request should be honored throughout the information supply chain, such as agreeing to remove an individual from a mailing list, for example. Increasingly, firms are required in many jurisdictions to provide, on demand, not just access but an account of all uses and disclosures of customer information.

Successful ONEs should strive to maintain and share only the most limited and accurate data or assessments about their customers with others, and should have in place mechanisms to deal with exceptions, corrections and other remedial processes. They should also take appropriate steps to ensure, and to demonstrate, that the networked sources from which they receive and supply customer data are reputable and trustworthy.

5.0 Technology

5.1 Context

Remarkable advances in information and communication technologies make it possible now, on a cost effective scale never seen before, to collect, store, process, and share vast amounts of highly granular personal data. This data becomes our digital shadow, proxies for the real thing, upon which organizations and governments alike will assess and make decisions both for and about us.

5.2 Privacy concerns:

Over collection and under disclosure (the law of unintended consequences)

Just because technology lets you do something, should you do it?

It is generally accepted that the development and adoption of new technologies races far ahead of our ability to understand their consequences, let alone control them. Perhaps this is a good thing, since it gives lead time for experimentation and innovation, and at times, unintended consequences.

Organizations that are early developers or adopters of innovative information communication technology (ICT) often stand to gain an advantage over their competitors, especially in new areas and industries. Being an industry pacesetter, however, sometimes comes at the cost of working in grey areas of regulation, and incurring hard to quantify privacy risks and public backlashes. All of the major ICT innovators of the past decade from Microsoft to Intel, Amazon, Google, eBay, and ChoicePoint have attracted their fair share of attention and criticism, not to mention regulatory scrutiny.

Sometimes companies can get too far ahead of the curve and trigger negative public reactions, either because the activity generates negative unintended consequences, or because it is offensive, or susceptible to exaggerated public fears. Privacy concerns are often dormant until shaken by a confluence of circumstances and developments.

Indeed, it is rarely technology itself that constitutes the privacy risk but, rather, the manner in which it is used by human decision-makers. For example, where some see utopian efficiencies, conveniences, and personalization in the deployment of RFID applications, others may see dystopian architectures of surveillance and control.

Consider the case of German retailer Metro, which in 2003 began an RFID trial in customer “payback” loyalty cards. Metro did not tell its customers what it was doing or why. When the RFID trial was discovered by accident, it generated a public backlash,

resulting in international boycotts that continue to this day.[34] The company's clumsy denials and public relations handling of the incident did little to assuage privacy concerns. Although no law was broken, trust in the large retail store operator was shattered. Metro eventually recalled the loyalty cards and replaced them with non-RFID versions, but the damage was done.

Compare this experience to that of ExxonMobil who, in 1997, developed the wireless payment application known as SpeedPass. Using RFID key fobs, six million consumers have utilized the payment option at 7,500 SpeedPass-enabled locations. The technology has been a great success, enabling Exxon to increase its customer satisfaction, retention rate, and market share.

Unlike Metro, Exxon's initiative was above-board; customers enrolled for the tags, clearly giving their informed consent. Secondly, the technology provided clear and demonstrable benefits to all customers allowing fast, convenient, secure payment at the pump obviated the need to produce and use a credit or debit card.

Right now, Metro and several other global manufacturers and retailers contemplating RFID deployment are busy contending with organized worldwide consumer boycotts and considerable attention from a broad range of government and regulatory agencies, privacy advocates, and consumer interest groups.[35]

ONE growth and success will be predicated on a virtually insatiable appetite for information. New technologies allow and even encourage the collection of ever more fine grained data about customers and their transactions that are then analyzed for insights and competitive advantage. What choices will firms make in the responsible use and deployment of technologies that can manipulate this data?

5.3 Digital footprints

Every time a cell phone is used, a website is visited, or a debit card swiped, a digital footprint is created. That digital footprint, pertaining to an identifiable consumer, is used by a company, or companies, to construct a profile of patterns and preferences which can then be used for promotion and marketing purposes.

These digital footprints are very valuable to marketing and advertising departments, and will become even more valuable in the future as tracking technologies improve and proliferate. Internet usage has become one of the most closely tracked activities in the last decade. It has even given birth to an entirely new industry of specialized customer tracking software.

34 "Customers say: We aren't your guinea pigs," Foebud.org <http://www.foebud.org/rfid/pressemitteilung/en>.

35 See, for example, Article 29 Data Protection Working Party, Working document on data protection issues related to RFID technology (January 1, 2005). International Conference of Data Protection & Privacy Commissioners, Resolution on Radio-Frequency Identification (November 20, 2003), FTC RFID Report (March 2005), and RFID Position Statement of Consumer Privacy and Civil Liberties Organizations (November 2003) at <http://www.privacyrights.org/ ar/RFIDposition.htm>.

In October 1999, an independent security analyst discovered that RealNetworks had assigned a global unique identification number (GUID) to each of its users who registered with its popular Real Jukebox software, and was using that number to track music listening patterns. Although RealNetworks claimed that the data were only used for aggregation purposes, GUID technology potentially enabled RealNetworks to create personal profiles that included everything from listening preferences to credit card numbers. This type of data collection was in direct contradiction to RealNetworks' stated privacy policy. The company subsequently amended its privacy statement to alert customers to the types of information that might be gathered, and released a software patch for users to block transmission of their personal information.[36] Angry customers, however, initiated two lawsuits against the company.[37]

Since then, consumer concerns and fears regarding clandestine online surveillance and data collection have continued to grow, and trust is continuously being eroded. Digital rights management technologies, for example, track and control online media usage with fine-grained precision. Similarly, spyware small software applications that surreptitiously install themselves on one's computer to track user activities has become a problem of epidemic proportions. U.S. lawmakers are wrestling with the spyware problem through appropriate legislative responses. In an effort to gather increasingly detailed information about online customers and generate metrics for marketing initiatives, many companies routinely insert "Web bugs" in their marketing email messages that report back when and how often the message was viewed, by whom, and what actions or links were followed. Very few people are aware of this now common online marketing technique; it is ripe for a privacy backlash or strong privacy self-defense techniques.

In sum, the overzealous or irresponsible deployment of invasive information and communication technologies can undermine the credibility of privacy promises and, in some instances, trigger strong consumer and legislative responses.

5.4 Possible solutions

The ONE must carefully consider the legal, public relations and economic risks of adopting any technology-enabled data collection strategy.

To start, it is important to recognize that much of the information that is collected is, in fact, personal in nature, meaning that it may lead to identifiability. Even if the information itself, such as a computer IP address, software unique ID, or shopper's card movements in a store is not personally identifiable per se, what matters is whether the data can be linked to an individual. In this context, firms should recognize and address the possibility that if they can collect this data, others may be able to do so too. For example, an RFID tag embedded in a loyalty card could also be read by competitors.

36 Courtney Macavinta, "RealNetworks changes privacy policy under scrutiny," C/Net, November 1, 1999 <http://news.com.com/RealNetworks+changes+privacy+policy+under+scrutiny/2100-1040_3-232238.html>.

37 Courtney Macavinta, "RealNetworks faced with second privacy suit," C/Net, November 10, 1999 <http://news.com. com/2100-1001-232766.html?legacy=cnet&tag=st.cn.1>.

It is important to limit collection to what is strictly necessary. Too often firms collect data simply because they can or because it has potential value.

It is very important to have clear privacy policies that are brought to the attention of the customer at the time of data collection. Firms should be very careful not to assume they know their customers' expectations and that "implied consent" has been given. If there are residual privacy and security risks, these should be noted and addressed.

Successful companies will always offer meaningful choices and controls to consumers, and invite their participation and feedback. For example, customers should be able to disable or control features or easily decline or uninstall unwanted software. And new technological deployments may be more readily accepted by consumers if there are clear, direct and demonstrable benefits, rather than general promises of improved administrative efficiency, personalized service, better choices and special offers.

Firms should make, and keep, their privacy promises. Doing so establishes credibility and trust over time, and helps to build the customer goodwill that will be necessary in the event of a privacy breach.

Lastly, firms should have a realistic crisis management plan. The successful ONE lives on the "bleeding edge" and must be ready for hard-to-quantify risks. Too often, ICTs are adopted and deployed without an adequate appreciation of the possibility of a privacy breach and the ensuing backlash.

6.0 Conclusions

The overarching theme relating to privacy in response to the Open Networked Enterprise is *accountability*. The successful ONE of the future may very well be global, decentralized, open, borderless, modular, flexible, empowering and so forth; characteristics that seem to reflect the Internet itself – but these same qualities challenge the responsible management of vast storehouses of customer information necessary for the ONE to succeed.

Remember to keep your focus on the customer. Taking a customer-centric view of information will highlight the distinction between personally identifiable information versus non personal information. The difference between how firms treat each is critical.

Identity Theft Revisited: Security is Not Enough

September 2005

Executive Summary

Identity theft is becoming one of the most serious current-day threats to the public, impacting millions of innocent people every year. The problem is becoming so widespread that we must all become vigilant against the abuses of our personal information. If victimized, however, a considerable amount of time and money may need to be spent repairing the damage to our credit and reputation. The problem has permeated so deeply into our daily lives that it has given birth to a new type of commercial enterprise — "identity theft insurance services," which are now being marketed to a wide range of individuals seeking greater peace of mind.

The recent outbreak of high-profile security breaches within the last year has had the unintended benefit of exposing long term problems in the way that organizations have been managing their customers' data. Consequently, this has drawn the attention and critical scrutiny of the public, shareholders, and lawmakers. As a result, a wide range of legislative responses are being proposed based on the growing support for the mandatory notification of data security breaches, and for imposing a measure of liability on firms who mismanage their customers' data.

The prevalence of identity theft comes about as a result of many complex factors. When examined closely, however, we believe that the single largest cause of identity theft is the existence of poor information management practices on the part of organizations. There is a growing belief that organizations that collect, use and share personal information should bear greater responsibility for actions which negatively impact the public, and should take preventative measures to ensure the privacy of their customers' data. Placing this problem at the foot of consumers and expecting them to "protect themselves" is somewhat akin to expecting a child to safely navigate his way across a highway of speeding cars – he wouldn't stand a chance.

While we identify several steps that consumers can take to minimize becoming a victim of identify theft, the problem is largely out of their hands. We place the problem in the hands of organizations that collect massive amounts of personal information and leave it largely unencrypted and in clear view of both insiders and outsiders alike.

This is a critical time for businesses to take the opportunity to review and improve their information management and security practices. This is necessary, not simply to avoid negative publicity and litigation, but also to build enduring trust with customers, partners and stockholders. In an effort to do so, businesses should consider the fundamental insights that data privacy can offer to organizational security – privacy and security go hand-in-hand.

The Problem of Identity Theft

Identity theft is the Crime of the Information Age, *the* Crime of the 21st Century – an unfortunate by-product of the growth and velocity of personal data coursing through vast, interconnected e-commerce databases and networks.

Today, every aspect of our lives is somehow affected and mediated by a number of digital devices such as credit cards, ATMs, cell phones, and computers. Communications and data transfers are no longer limited to our place of work; they are now on our persons, in our cars, in our homes. As a result, through the use of various technologies, we invariably leave behind a lengthy trail of digital footprints.

From these digital tracks, others can reconstruct our digital histories, and with these data dossiers, map out who we are, what our interests and opinions are, who our friends are, where we have been, and predict where we will be going. With fewer face-to-face transactions and more remote automated decision-making, the potential to misuse these digital footprints can profoundly affect our lives by those who gather our data both openly, and indirectly.

Identity theft involves the use of a victim's personal information to impersonate them and illegally access their accounts, obtain credit and take out loans in the victim's name, obtain accommodation, or otherwise engage in transactions by masquerading as the victim. Identity theft also includes the acquisition or transfer of personal information as an instrument to commit these crimes in the future.

According to the U.S. General Accounting Office: "Identity theft or identity fraud generally involves 'stealing' another person's personal identifying information … and then using that information to fraudulently establish credit, run up debt, or take over existing financial accounts."[1]

The IPC recognizes that there are significant differences between identity *theft* and identity *fraud*. True identity *theft* occurs when someone uses your personal information – such as your Social Insurance Number or Social Security Number, birth date, mother's maiden name – to impersonate you and apply for new credit accounts in your name. Identity *fraud* typically involves an unauthorized person using your credit card number from an existing account to make purchases. For the purposes of this paper, which focuses upon the information management practices of organizations that collect, use and share personal information, we will use 'identity theft' to refer to both.

Identity theft is the fastest growing white collar crime of the past decade, and the number one U.S. consumer complaint. A 2003 Federal Trade Commission survey estimated

1 U.S. General Accounting Office, *Identity Theft: Greater Awareness and Use of Existing Data Are Needed*. Washington, DC., June 2002, Document #GAO-02-766, p.23: **www.consumer.gov/idtheft/reports/gaod02766.pdf**. The U.S. Federal Trade Commission has adopted a similar definition, i.e.: "Identity theft occurs when someone uses your personal information such as your name, Social Security number, credit card number or other identifying information, without your permission to commit fraud or other crimes." See **www.consumer.gov/idtheft/**.

that nearly 10 million Americans were victims of some form of ID theft within the past year, triple the number in 2001.[2] According to survey data released in July 2005 by Chubb Insurance, 20% – one in five – Americans has been a victim of identity theft or fraud.[3]

A recent survey conducted by Privacy and American Business ("P&AB") and Deloitte Touche found that 20% of respondents reported having been a victim of identity fraud or theft.[4]

Dr. Alan Westin, one of the foremost privacy experts and publisher of Privacy & American Business, commented: "Our survey shows that there does not seem to be a plateau as yet in the instances of identity theft, despite major attempts by business and government to stem the tide."[5]

Identity theft can and does take many forms. Personal information itself is sometimes used to obtain more detailed information on a targeted victim, and the methods are constantly changing. Computer viruses, "Trojan horses," "worms," keyloggers, and other malicious spyware, capable of harvesting personal information from the computers of unsuspecting owners and then "phoning home" with the data, have become an epidemic.[6] "Phishing" and "pharming" are the latest techniques, whereby scammers electronically masquerade as legitimate businesses, contact innocent accountholders, and request confidential data such as account numbers and passwords.[7] The techniques are constantly mutating: rather than posing as a bank or other online business, "spear phishers" send e-mail to employees at a company or government agency, making it appear that the e-mail comes from a powerful person within the organization. Once they trick employees into giving up passwords, they can install malicious software programs that ferret out additional sensitive information or secrets.[8]

Contrary to the popular myth that identity theft and fraud are carried out using high-tech methods by renegade computer geniuses, the fact remains that these crimes continue to depend on a steady and easily accessible supply of personally identifiable information (PII).

2 Federal Trade Commission, *National and State Trends in Fraud & Identity Theft, January–December 2004*, February 1, 2005, **www.consumer.gov/sentinel/pubs/Top10Fraud2004.pdf**.

3 Chubb Insurance, news release: "One in Five Americans Has Been a Victim of Identity Fraud", July 7, 2005 **http://www.chubb.com/corporate/chubb3875.html** See also Ipsos-Reid, "Concern About Identity Theft Growing in Canada" survey results at: **www.ipsos-na.com/news/pressrelease.cfm?id=2582**.

4 Privacy & American Business and Deloitte & Touche LLP, *New Survey Reports An Increase in ID Theft and Decrease in Consumer Confidence*, Survey results released June 29, 2005 available at: **www.pandab.org/deloitteidsurveypr.html**.

5 Ibid.

6 See, for example, Ingrid Marson, "Identity theft ring affects at least 50 banks" in ZDNet, August 08, 2005 For more information on spyware see **www.cdt.org/privacy/spyware/** For an inventory of spyware bills and similar legislation, see **www.benedelman.org/spyware/#legislation**.

7 For more information see **www.antiphishing.org**.

8 Reuters, "Online Scammers Pose as Execs in 'Spear-Phishing' " reported in eweek.com, August 17, 2005 at **www.eweek.com/article2/0,1895,1849431,00.asp** See also **http://en.wikipedia.org/wiki/Phishing**.

Normally referred to as "tombstone data," information that is stolen by identity thieves includes a person's name, home address, account number, credit card information, social security/insurance number, driver's licence number, date of birth, mother's maiden name, passwords, and other personal details. Armed with enough personal data, identity thieves can take on many different "financial personas."

To put some perspective on just how little an identity thief needs to work with, research conducted at Carnegie-Mellon University determined that nearly 90% of the U.S. population could be uniquely identified through the use of only three pieces of information: a person's date-of-birth, sex, and postal code.[9]

Victims of ID Theft: The Consequences

In most cases, victims of identity theft have absolutely no idea they have become victims until it is usually too late. Out of the blue, the victim may find herself denied a purchase or a loan, denied a credit limit increase, or even denied an apartment rental – almost anything that involves a credit or background check. And then her life changes.

The effects of identity theft can be truly devastating. "Data rape" leaves deep scars on victims and consumes a significant amount of their time and effort. A great deal of time may be expended in persuading banks and credit bureaus to remove fraudulent accounts from their credit reports, or convincing creditors to stop reporting them as defaulters and deadbeats.

Unpaid debts and collections can ruin a victim's credit score and creditworthiness, often leading to denials of mortgage and other credit. As the aggravation and frustration compound, the burden remains on the victim to write certified letters, keep detailed records and follow up with companies until the problem is resolved. Identity theft victims typically spend hundreds of hours, and dollars, in their efforts to clear their names.

Consumer Education and Awareness Efforts

Growing recognition of this epidemic has prompted consumer groups, government agencies, and business organizations to introduce consumer education and awareness efforts and to provide some measure of support for victims and others at risk. The advice typically takes two forms: one, a helpful collection of advice and tips on how to minimize the risk of becoming a victim; and two, advice and resources on what to do, and where to go, upon becoming a victim.

As consumers, we are told to be careful about disclosing and discarding our personal information, to buy shredders, avoid dumpster divers, select hard-to-guess passwords (and change them frequently), be careful of whom we do business with, read privacy policies, request copies of our credit reports each year, and generally, minimize the amount of personal information we divulge, intentionally or otherwise. (See Consumer Help Tips section below.)

9 L. Sweeney, "K-Anonymity: A Model for Protecting Privacy," *Int'l J. Uncertainty, Fuzziness, and Knowledge-Based Systems*, vol. 10, 2002, pp. 557–570.

The underlying theory behind helpful tips seems to be that if people become more vigilant, arm themselves with these remedial powers,[10] and take suitable precautionary steps, the risks and effects of identity theft can be significantly minimized. **We do not agree.**

Given the epidemic nature of the problem and the clear harm it bears upon victims, it shouldn't be too difficult to persuade people that it is in their own self-interest to be vigilant about their personal information, their identity, and their credit histories. But this approach can be very misleading because it suggests that individuals can prevent the occurrence of this problem. For the most part, they cannot.

Don't Blame the Victim

Daniel Solove, a law professor at Georgetown University, has pointed out the problems that arise when individuals are expected to "take control" of their own digital dossiers, and exercise any rights available to them. Professor Solove points out that personal data is often collected unwittingly, without one's consent.[11] In the United States, a social security number (SSN) is a necessity of life in society and is vital for many activities from employment to renting an apartment. Refusal to give out one's SSN can result in much inconvenience and ultimately, the absence of services being provided. A credit report can be used in lieu of the SSN, but most people cannot even name the major credit reporting agencies, let alone know how to request copies of their credit reports. Even if someone did take this cautionary step, the risks are still out there and not necessarily minimized to any significance. "There is no way you can fully immunize yourself from identity theft because the information is, and always will be, out there."[12]

The Real Problem

While individuals may contribute to the growth of identity theft, their involvement in its prevention is, in our view, minimal. The incidence of identity theft has skyrocketed largely because of poor information management practices by organizations, especially relating to data storage and retention, coupled with the explosive collection of personally identifiable information (PII). Most PII collected is retained in clear text (thus in plain view), meaning that the data is not encrypted or encoded in any way, nor are the personal identifiers severed or separated from the data itself. Therein lie the biggest problems – poor information management practices, poor security, and poor data storage practices.[13]

10 Such as requirements for informed "affirmative" consent as well as data access and correction rights.

11 Solove, Daniel J., Identity Theft, Privacy, and the Architecture of Vulnerability, Hastings Law Journal, Vol. 54, p. 23, 1227, 2003, p. **http://ssrn.com/abstract=416740**.

12 Ibid, p. 23

13 The problem of identity theft is further exacerbated by widespread poor authentication practices of businesses that allow fraudsters to make purchases, open new accounts, and obtain credit, etc. "Pre-approved credit card offers" are perhaps the most well-known example. Some industries (debit-card, cell phone) write off the costs of bad accounts as an acceptable cost of doing business – see discussion in report of Consumer Measures Committee, Working Together to Prevent Identity Theft - A Discussion Paper (July 2005) esp. pp. 6-7.

Professor Solove adds: "The identity thief 's ability to so easily access and use our personal data stems from an architecture that does not provide adequate security to our personal information and that does not afford us with a sufficient degree of participation in the collection, dissemination and use of that information."[14]

While certainly not new, the data security problem has only recently come into the spotlight. A comprehensive study of 4,000 U.S. businesses reported that more than half of them had suffered database security breaches in the past year.[15]

It is one thing to have someone pilfer through your mail, or your unshredded trash, looking for credit card records, receipts and statements to steal, but quite another when electronic databases are involved. The identity theft problem becomes considerably magnified by the widespread sharing, selling, trading, matching, accessing, copying, misuse and outright theft of large databases containing hundreds of thousands of detailed customer files. Why steal one identity when you can steal thousands of them, remotely, and without detection?

The Incidence of Identity Theft: Recent Examples

A recent string of major data security and privacy breaches resulting from loss, theft, insider abuse, and fraudulent access have thrust the issue of responsible personal information stewardship into the realm of the public, lawmakers, and the media.

Examples of recent security and privacy breaches include:

- June, 2005: CardSystems Solutions Inc, a firm that processes credit card transactions for MasterCard, Visa, American Express, and Discover, reported that hackers had stolen 40 million credit card numbers. CardSystems' CEO admitted that the company should not have been retaining consumer credit information that was compromised as a result of a hack. In violation of its service agreements with the credit associations, CardSystems had kept information on approximately 200,000 credit accounts for research purposes.[16]
- June, 2005: Citigroup reported that personal information on 3.9 million consumer lending customers of its Financial subsidiary was lost by UPS while in transit to a credit bureau. The data on the backup tapes were not encrypted.[17]
- May, 2005: Media giant Time Warner reported that it lost a container of computer tapes with company data including the names and Social Security numbers of 600,000 U.S. employees and their dependents. The backup tapes were not encrypted.[18]

14 Ibid, p. 24

15 Cf. CSI/FBI Computer Crime and Security Surveys, available at **http://www.gocsi.com/**.

16 See news coverage at: **www.msnbc.msn.com/id/8260050/** and **www.msnbc.msn.com/id/8286132/**.

17 See news coverage at: **http://money.cnn.com/2005/06/06/news/fortune500/security_citigroup/**.

18 See news coverage at: **http://money.cnn.com/2005/05/02/news/fortune500/security_timewarner/**.

- May, 2005: The U.S. Department of Justice reported the theft of a laptop computer containing travel account and credit information for as many as 80,000 Justice employees. The data on the laptop was protected by a password.[19]
- April, 2005: Online brokerage Ameritrade disclosed that it had lost a backup computer storage tape containing records for 200,000 of its customers. The tape was lost in transit. The data was stored in plain text format, unencrypted.
- April, 2005: Global Bank HBSC notified at least 180,000 people who used GM MasterCard credit cards to make purchases at Polo Ralph Lauren to replace their cards because criminals may have obtained access to their credit card information. The issue was confirmed as a technology-related problem; Polo said that the credit card data in question was inappropriately stored in its point-of-sales software system.[20]
- April, 2005: DSW Shoe Warehouse reported that hackers had accessed data on 1.4 million credit card transactions and another 96,000 processed cheques in more than 100 stores over 25 states over a three month period starting in February 2004.[21]
- April, 2005: A California medical group notified 185,000 current and former patients that their financial and medical records may have been compromised following the theft of computers containing personal data. The theft occurred after the group copied plain text patient and financial information from its secure servers to two local PCs as part of a patient billing project and year-end audit.[22]
- April, 2005: A former employee of a Washington-area Blockbuster video store was indicted on charges of stealing customers' identities, and using them to buy more than $117,000 in trips, electronics, and other goods, including a Mercedes-Benz car.[23]
- March, 2005: Health care giant Kaiser Permanente notified 140 patients that a disgruntled former employee had posted confidential information about them on her Weblog. The health care giant learned of the breach indirectly in January, 2005, from the federal Office of Civil Rights.[24]

19 See news coverage at: **www.washingtonpost.com/wpdyn/content/article/2005/05/31/AR2005053101379.html**.

20 See news coverage at: **http://news.com.com/2061-10789_3-5672286.html?part=rss&tag=5672286&subj=news**.

21 See news coverage at: **http://searchsecurity.techtarget.com/columnItem/0,294698,sid14_gci1081866,00.html** and **www.informationweek.com/story/showArticle.jhtml?articleID=161601930**.

22 See **http://judiciary.senate.gov/testimony.cfm?id=1437&wit_id=729**.

23 See news coverage at: **www.washingtonpost.com/wp-dyn/content/article/2005/04/25/AR2005042501411.html**.

24 See news coverage at: **www.networkworld.com/news/2005/0316kaiseperma.html?nl**.

- March, 2005: Time Warner Inc. reported that computer tapes containing the names, SSNs, and other personal data of 600,000 current and former employees were lost during their delivery to a data-storage facility in March, 2005. “The information on the tapes is in a form that's not easily accessed,” stated a company spokesperson. Time Warner later publicly adopted a recommendation and new policy that all backup tapes be encrypted.[25]

- March, 2005: LexisNexis reported a privacy breach in its database division, where hackers accessed more than 300,000 profiles, including SSNs and drivers licence numbers, more than 10 times the number originally reported. Poor computer access management practices –mainly stolen passwords– were blamed.[26]

- March, 2005: A thief had stolen a laptop with personal information on 100,000 University of California, Berkeley alumni, graduate students and past applicants. The information, including names, SSNs, and in some instances birth dates and addresses, was unencrypted, although the laptop was password-protected.[27]

- March, 2005: Boston college officials warned 120,000 alumni that their personal information may have been stolen when an intruder hacked into a school computer containing the addresses and SSNs of college graduates. The computer system was not run by the school, but by an outside contractor, for looking up the names and phone numbers of graduates in order to solicit donations.[28]

- February, 2005: Bank of America confirmed it had lost backup tapes containing the personal information of 1.2 million federal employees. Some of those records contained information about senior U.S. congressional representatives. The data on the missing tapes were not encrypted.[29]

- November, 2004: Data broker ChoicePoint, having built a $1 billion annual business around their “core competency of verifying and authenticating individuals and their credentials,” reported the unauthorized access of over 150,000 detailed records by scam artists over a period of one year. At least 700 known instances of identity theft resulted from this security breach. Poor access control and authentication procedures were blamed.[30]

- November, 2004: A major Canadian bank – the CIBC – repeatedly sent confidential customer files by fax to a U.S. junkyard over a period of several years, despite

25 See news coverage at: **www.boston.com/business/technology/articles/2005/05/03/snafu_puts_600000_at_security_risk/**.

26 See April 12 press release, *LexisNexis Concludes Review of Data Search Activity, Identifying Additional Instances of Illegal Data Access* available at: **www.lexisnexis.com/about/releases/0789.asp**.

27 See testimony at **http://judiciary.senate.gov/testimony.cfm?id=1437&wit_id=729**

28 See news coverage at: **www.msnbc.msn.com/id/7221456/**.

29 See coverage at: **www.theregister.co.uk/2005/06/07/citigroup_lost_tape/** and **www.msnbc.msn.com/id/7032779/**.

30 For a thorough chronology, see EPIC’s ChoicePoint web page at: **www.epic.org/privacy/choicepoint/**.

being advised on many occasions by the junkyard owner, of the incorrect fax number and the transmission of sensitive personal data.[31]

- Other security breaches have occurred due to small automated errors in the management of databases that can quickly become amplified into major security breaches, such as disclosure of drug users in the "To" (instead of Bcc) line of a marketing or communication email message. The "classic" example of this type of privacy breach involved pharmaceutical giant Eli Lilly, who in 2001 accidentally disclosed the e-mail addresses of 669 subscribers to its Prozac Reminder Service.[32]

Customer Data is Cheap but Valuable

The Perfect Privacy Storm: The recent security scandals have brought to the surface the extent of personal information being collected and used by businesses in an effort to "know their customers better," to predict their behaviour, and to make decisions about them.

Each time someone uses a cell phone, visits an internet site, turns on a cable TV service or swipes a credit, debit or loyalty card, they leave behind a digital trail. Companies track these trails for patterns and preferences, constructing personal profiles, which companies can then use to promote new products or target advertising to specified customers.

Digital footprints are valuable to advertisers and marketers, and will become even more so as tracking technologies continue to advance. Internet usage has become one of the most closely tracked activities in modern life, with dozens of companies specializing in selling software services that can track an individual customer as he or she moves around the Net, compiling a snapshot of their interests that can then be sold to advertisers. This information can then further be matched or compared with records about customers found elsewhere, to create new profiles and assessments of shopping habits.

Thanks to new information technologies and services, it is now more possible than ever for businesses to "know their customer." There is nothing wrong with this practice provided that the customer wants to be known, by having consented to the relationship. This may or may not happen. Companies routinely collect personal data from third parties, often in near real-time, to carry out background and reliability checks, to authenticate claims, and to develop a more comprehensive and intimate understanding of their customers. More and more of these types of "history" checks are being carried out in real-time to minimize business risks by assessing creditworthiness, health conditions, insurance claims history, purchases, lifestyle patterns, and so forth.

31 See factual account by Privacy Commissioner of Canada, "CIBC's privacy practices failed in cases of misdirected faxes" report of April 18, 2005 at **www.privcom.gc.ca/incidents/2005/050418_01_e.asp** and addendum at: **www.privcom.gc.ca/incidents/2005/050418_02_e.asp**.

32 See FTC report and settlement of April 18, 2003, "Eli Lilly Settles FTC Charges Concerning Security Breach" at **www.ftc.gov/opa/2002/01/elililly.htm**.

The emergence of these digital files has become the subject of intense debate about regulatory oversight. The amount of information being collected and traded in this new "infomediary" industry is estimated to be worth approximately $10 billion per annum.

In the wake of numerous high-profile customer-data breaches, companies that have not previously been subject to information security and privacy regulation should expect new regulations to mirror elements of existing laws. For example, following California's landmark *Database Breach Notification Security Act* ("SB1386"), which requires notice to be given to consumers of breaches in security of data held by a business or government agency, 18 other states have passed similar security breach notification laws in 2005, with numerous other security breach notification bills pending in other states (16 at last count). In addition, a number of breach notice bills have been introduced and are progressing at the federal level.

Other bills being contemplated at the state and federal levels in response to the security breaches and identity theft problems have provisions that seek to restrict certain organizations' ability to collect, use and share personal information, to strengthen prior notification and consent requirements, and to enhance the access and redress rights of individuals vis-à-vis those organizations.

From a privacy perspective, it is somewhat unnerving that these large databases are held by third parties that have no direct relationship with the people whose information they possess, nor any obligation to provide data access or correction to those persons, yet this appears to be occurring with greater frequency.

As Information and Privacy Commissioner, I have been publicly calling upon the provincial government to introduce comprehensive private-sector privacy legislation. In light of the recent rash of security breaches, the poor information management practices those breaches have exposed, the epidemic of identity theft, and the eroding trust and confidence that consumers have in organizations to manage their personal information responsibly, I have renewed my call for private sector legislation that can serve the interests of both consumers and businesses alike by establishing an effective framework for transparency, accountability and trust.

For businesses that wish to start their planning, there's no need to wait for implementation instructions on how to secure consumer data – start now!

Data Assets = Data Risks and Liabilities

What is becoming abundantly clear is that when customer data begins to haemorrhage due to a company's negligence, it is customers who often suffer the most, in the form of financial losses, identity theft, poor credit ratings, etc. Innocent individuals end up paying the price for careless data security practices of organizations. That is to say, the negative externalities or costs of bad security practices are often borne not by the host organization, but rather by the customers themselves.

The lack of compelling risk and liability for businesses has led some to speculate that organizations lack strong economic incentives to invest in good data privacy and security practices.[37] If data security breaches need not be reported, and the cost of those breaches is largely borne by others (with little likelihood of causally connecting the breach to the resulting harm), then companies have few reasons to address the data privacy and security problem in a systemic way. Further, if the expense of dealing with privacy breaches is minimal compared to the overall bottom line, then there may be few incentives to address data privacy and security seriously; losses due to fraud and identity theft may be tolerated as the "cost of doing business."

To cite an example of the above, an investigative report was conducted to determine why Canadian banks still use ATM cards (with magnetic strip technology), which are increasingly becoming vulnerable to identity thieves. The alternative to magnetic stripe cards are "smart cards" which are implanted with a computer chip that uses encryption to protect the information, thus making them far more secure from identity theft. So, the question was asked: why are banks not embracing "smart card" technology? The primary reason would appear to be cost. In 2003, bank experts estimated that it would cost Canada's banking industry $500-million to produce and implement the new "smart card" technology for the debit card system, while debit card fraud only costs $44-million in comparison."[38] Simply put, financially, it would appear that it is less costly for banks to assume the cost of identity theft than to implement a new, more secure system. Yet, there is growing recognition that it is unreasonable to have the burden and responsibility for vigilance placed upon the consumer when the vulnerabilities and risks are largely generated not by themselves, and at times, by unknown third parties.

Some laws and regulations do impose a "duty of care" on businesses to collect and manage sensitive personal information in special ways, such as to provide notice, obtain consent, and to provide access and correction rights. In the United States, the Health Insurance Portability and Accountability Act features data security requirements for electronic health data; Sarbanes-Oxley imposes responsibilities on publicly-traded companies to establish and maintain adequate internal controls over information systems, as well as an assessment of the effectiveness of those internal controls; Gramm-Leach-Bliley requires firms to ensure data privacy for consumers; the *Fair Credit Reporting Act* and the *Fair and Accurate Credit Transactions Acts* prescribe conditions for collecting and managing personal financial information, such as those contained in credit scores.

However, there are additional reasons for businesses to demonstrate greater care in guarding their customers' personal information against identity theft. Rena Mears, leader of the Privacy Services Group of Deloitte & Touche, made an astute observation:

37 See, for example, Ross Anderson, Why Information Security is Hard - An Economic Perspective, 2001, at **www.ftp.cl.cam.ac.uk/ftp/users/rja14/econ.pdf** and Jean Camp, et alia, **www.infosecon.net**.

38 CTV News, W-Five, "Debit Card Fraud", January 8, 2005.

> "There is a significant portion of the population that is becoming concerned about identity theft, and it is influencing their purchasing decisions. Companies need to understand this and leverage the internal control improvements they have made as a result of Sarbanes-Oxley to increase the integrity and security around the personal information they hold for their customers."[39]

As noted earlier, the recent security breaches have sparked an explosion of public concern about the current data management practices of businesses. The majority of the security breach notification bills introduced at the state and federal levels are modelled after California's SB1386, and require companies to notify individuals when their personal information has been lost or stolen. These new laws, when they come into force, will serve as a powerful stimulus to enhance the privacy rights of individuals. Had it not been for this one requirement to notify affected customers, the revelation of the ChoicePoint incident and other breaches that followed would most likely never have become a matter of public knowledge.

Beyond notification of security breaches, an inferno of other federal and state legislative activity has developed across the United States. As of May 2005, there were 39 bills pending in 19 states proposing to regulate the use of personal information, with other bills responding to the growing privacy threats stemming from spyware, phishing, pharming, and other Internet-related threats. This movement has also fuelled other privacy firestorms. In addition to the above 39 bills, there were an additional 115 bills, pending in 40 states, that are seeking to protect and safeguard personal information when it comes to the data industry and overseas outsourcing.[40]

Transparency and accountability are fundamental privacy principles. Privacy laws typically seek to effect these principles in statute and regulation, usually going farther to prescribe rules and conditions for the collection, use, and disclosure of personal information by organizations, and to provide certain rights to individuals vis-à-vis those organizations that would collect and use their data. Privacy laws are usually based upon a widely recognized set of *Fair Information Practices* (FIPs), which we discuss later in this paper.

There is a fundamental change underway towards greater transparency and accountability by organizations and their practices of data management, assurances of security, and handling of information assets. What was once a competitive strategic marketing decision is becoming a regulatory baseline and market imperative. Poor or opaque information management practices, when exposed, and if serious, are provoking adverse consequences in the form of fines, lawsuits, public backlashes, damage to brand and reputation, lost business, growing penalties, and other containment costs.

Customers and lawmakers alike are demanding stronger remedies whenever wrongful, or negligent action involving their personal information takes place. According to a

39 Cited in Privacy & American Business and Deloitte & Touche LLP, *New Survey Reports An Increase in ID Theft and Decrease in Consumer Confidence*, June 29, 2005 at: **www.pandab.org/deloitteidsurveypr.html**.

40 Briefing from Privacy & American Business, *Privacy Legislation in the States.*

Privacy & American Business study, since 2000, 182 cases of consumer privacy litigation have been brought against 234 U.S. businesses, which have paid out more than $160 million in fines and penalties due to privacy and security litigation.[41]

Increasing awareness among the public and lawmakers is driving the growth of strong privacy management practices: "The need for proper privacy management is increasing, and U.S. businesses must implement more robust customer privacy policies now or face government intervention and severe customer backlash."[42] Organizations can mitigate business and legal risks by adopting a high standard of *proactive* data privacy and information management into their operations, and consistently demonstrating compliance with those standards.

One recent example of a proactive approach comes from Microsoft. In April 2005, Microsoft filed 117 "John Doe" lawsuits in the U.S. against suspected "phishers" hoping to catch some of the biggest offenders. The accused were allegedly trying to con people out of sensitive personal information, such as bank details, passwords, and social security details, by using fake MSN, Hotmail accounts and websites, and mass e-mail and pop-up ads. Because there is no specific anti-phishing legislation in the United States, the lawsuits were filed in the U.S. District Court in Seattle under the *Lanham Act*. This is a federal trademark protection law that carries a maximum of US$1 million fine per violation.

However, this issue involves much more than mere compliance. If you treat privacy as a business issue, and think about it strategically, you will go much further to discovering a competitive advantage. "How can this legal problem create an opportunity to gain an advantage over one's competitor?" was the question asked in *Using the Law for Competitive Advantage* by George J. Siedel.[43] The answer lies, in part, in adopting comprehensive data privacy standards that can build enduring trust and loyalty.

One way to accomplish this is by applying the Fair Information Practices in a more comprehensive and rigorous manner than before. Professor Fred Cate, a leading U.S. academic and public commentator on information law, observed that, "The greatest failure of FIPPS [Fair Information Practice Principles] as applied today is the substitution of maximizing consumer choice for the original goal of protecting privacy while permitting data flows … Compliance with data protection laws is increasingly focused on providing required notices in proper form and at the right time, rather than on ensuring that personal information is protected."[44]

41 Briefing from Privacy & American Business, *Consumer Privacy Litigation.*

42 Walter Janowski, Research Director, Gartner , 19 May 2003. See **www.gartner.com/5_about/press_releases/pr19may2003a.jsp**.

43 *Using the Law for Competitive Advantage*, George J. Siedel.

44 Cate, Fred H., "The Failure of Fair Information Practice Principles," forthcoming in *Consumer Protection in the Age of the 'Information Economy',* a draft manuscript for a forthcoming book. Quoted with the author's permission.

What guidance can data privacy provide to security professionals tasked with securing large customer databases from SB1386 and similar breach notification laws? Read on.

Data Privacy = Good Data Security

Privacy is *Holistic*: Develop a Culture of Privacy

Like the best security practices, data privacy is comprehensive in its approach to protecting personal information. Although privacy always applies to individual data items ("any information about an identifiable individual"), it also takes into account a much broader environment. Data privacy asks principled questions at every step of the information lifecycle, from collection and use through to disclosure and disposal.

The Office of the Information and Privacy Commissioner of Ontario offers useful information tools and privacy management documents on its website, **www.ipc.on.ca**, to help organizations improve their privacy practices and policies:

- map data assets, current flows and uses;
- carry out privacy gap, threat and risk analyses;
- carry out privacy impact and risk assessments;
- plan and execute a successful privacy program;
- build privacy into information and consumer technologies;
- adopt leading-edge best practices; and
- build strong consumer trust and loyalty.

Summary: "Put someone in charge, analyze vulnerabilities, make a plan, implement policies and procedures that address technology as well as business processes, train, monitor your service providers, and continually revolve back to evaluate and adjust your program on an ongoing basis."[45]

It is also important to remember that privacy is not the responsibility of one division, department, branch, manager or executive. All organizations, both public and private, need to implement a multi-purpose privacy team made up of members from across the entire spectrum of the organization. You need to develop a culture of privacy. Privacy is more than just an organizational contingency, it is a mindset – a way of thinking. Remember that while technology may look good, your customers don't interact with your technology. It will always be organizational behaviour that gains the trust of consumers.

Fair Information Practices

The comprehensive management and systemic approaches of privacy are evident in a basic set of principles called Fair Information Practices that form the foundation of all privacy laws and policies. In Canada, the 10 principles contained in the Canadian

45 Stampley, Dave, *Three Ways to Prepare for the IT Impact of New Privacy Laws*, InformationWeek, May 2, 2005: **www.informationweek.com/story/showArticle.jhtml?articleID=161600945**.

Standards Association *Model Code for the Protection of Personal Information*[46] are as follows:

> **Accountability** – *an organization is responsible for personal information under its control and shall designate someone who is accountable for the organization's compliance.*

Without basic accountability, there is little possibility of learning about security breaches, and no chance of taking appropriate remedial actions. A big part of the spam, phishing, pharming, and spyware problems, is the difficulty in establishing the source of the originator and holding them accountable.

"It's really only because of the California law that we now know," noted U.S. Senator D. Feinstein, sponsor of a federal data breach notification bill that would "require any agency or company that collects personal information to notify potential victims of identity theft when a security breach is discovered; impose a fine of up to $50,000 per day for each day that a company fails to notify victims about unauthorised access to personal information."[47]

Tyler Hamilton, a renowned author and columnist on technology and the law, noted that "forcing companies to disclose privacy breaches right away gives victims a chance to fight back within a reasonable time."[48]

The presence of an accountable privacy officer provides an avenue for victims to seek correction to mistakes and errors and, in general, to seek redress.

> **Identifying Purposes** – *the purpose for which personal information is collected shall be identified by the organization at or before the time of collection.*

The practice of indiscriminately and excessively collecting personal information, on the theory that stockpiling the data is cheap and may yield new insights that would become valuable someday, will be increasingly called into question. Collecting more information than you need may, and in the future, will most likely expose your organization to greater liability and risk.

Strong privacy practices help to discipline the collection of personal information at the very start of the information lifecycle by requiring purposes to be specified in advance. If the purposes are clearly stated and made known to the individual at the time of the collection, that leads to a stronger basis for "choice" and "consent."

46 See **www.csa.ca/standards/privacy/Default.asp?language=english** .

47 Senate Takes up Data Security Law, Internet News, June 16, 2005 at **www.internetnews.com/security/article.php/3513201** and April12, 2005 at **www.internetnews.com/bus-news/article.php/3497161**. See also **http://feinstein.senate.gov/05_releases.html**.

48 Tyler Hamilton, "Web, databases feed identity theft", The Toronto Star, Dec. 9, 2002 at **www.tecrime.com/llartl16.htm**.

In addition, overly broad purposes such as "to improve customer service," or "to ensure security," will need to be justified in greater detail, particularly when a breach has occurred and questions of informed consent are raised.

> **Limiting Collection** – *the collection of personal information shall be limited to that which is necessary for the purposes identified, and collected by fair and lawful means.*

On the general theory that "more data is better," indiscriminate and excessive collection of personal information by organizations is a disturbing trend. But the more information that is collected, the greater the chances that some of it will be inaccurate and out of date. Depending on where the data came from and how it was acquired, there is a greater likelihood that it may have been collected by unlawful means – exposing firms to charges of deceptive business practices and breaches of contract. Further, collecting more information than is necessary for specified purposes may aggravate customers, and result in a loss of business.

> **Limiting Use, Disclosure, and Retention** – *Personal information shall not be used or disclosed for purposes other than those for which it was collected, and shall be retained only as long as necessary for the fulfillment of those purposes.*

Unauthorized disclosures and secondary uses of personal information stored in large databases is in many cases the central problem contributing to identity theft.

The solution to this problem is to minimize your risk and liability by limiting not just the collection, but the use, disclosure and retention of personal information in the care and custody of the host organization.

This can be relatively straightforward as in deciding not to collect personally identifiable information in the first place, or deciding to configure cash register receipts to mask or truncate portions of credit or debit card numbers on printouts. It might mean configuring internal networks and software clients to withhold or mask the transmission, or display of sensitive and unnecessary fields such as driver's licence numbers, to frontline customer relations staff.

If the purpose of collecting sensitive personal data from the customer is to carry out a credit check to assess their creditworthiness, then there may be little need to retain this data once the assessment has been made. The same concept applies to sensitive personal information collected from background checks and interviews of potential employees. Once the purpose is fulfilled and a decision has been made, the data should be purged from the system, after allowing for the possibility of challenge to the final decision. As long as sensitive personal information is kept past its expiry date, it will always represent a potential risk and liability.

Further, if the purpose of collecting sensitive personal data is to authenticate the customer or subscriber when that customer requests an account change, then any "common secret" should suffice instead of "open secrets" like mother's maiden name or SSN/SIN numbers. Wherever possible, authenticating a customer in person should not involve making a permanent photocopy or record of personal documents.

Retention and destruction schedules for customer information, regardless of storage format, should be an integral and verifiable part of any organization's data management system. Document destruction policies for physical and electronic media should be developed and distributed to all involved in the processing of customer data. The use of shredding for physical records and wiping or other permanent forms of destruction for electronic media should be strongly encouraged. Adherence with these policies should be closely monitored and verified. Preferably, the destruction schedule should be an automatic process to maximize the control of potential risks.[49]

Privacy should be viewed as a security improvement for all stakeholders. Data privacy builds customer trust; business privacy protects stockholder equity.

Privacy is *Personal*: Consider the Individual's Interests

While security and privacy share some important common qualities and features, security is *not* privacy. IT security professionals often make the mistake of believing that if customer data can be kept confidential and preserved from corruption, then privacy is guaranteed. [*See IPC "Privacy vs. Security: Common Misconceptions"*]

Security tends to look at information management practices from a top-down control perspective in an effort to protect company data, processes and systems from attackers. Privacy, on the other hand, protects the interests of the *individual*. Its central focus is to restrict the use of an individual's data to the purposes specified – the emphasis is on containment, not widespread use throughout the organization.

Information security typically refers to the controls deployed by an organization for the purposes of securely collecting, using, and holding all data. It applies to personal and nonpersonal data alike. Privacy protection, conversely, applies only to personally identifiable information and focuses on how the interests of the identifiable data subject — the person providing the information — are affected. Depending on the type of business, this may describe either a major portion of the data held by an organization, or only a small segment.

In another comparison, the Chief Security Officer (CSO) tries to optimize *organizational control*, often starting from a security perimeter mentality. The Chief Privacy Officer (CPO) on the other hand, seeks to maximize *personal control*, to ensure that the individual maintains control over their personal information and that authorized users do not misuse their data.

49 Ann Cavoukian, Ph.D., "Privacy: Strong Information Practices are a Must – From Collection to Destruction.", NAID News, September 15, 2005.

There is growing support for strengthening privacy practices that allow individuals to exercise greater control over the accuracy, completeness, timeliness, use, distribution and disposition of their own personal information. For example, U.S. identity theft victims can now obtain free copies of their credit reports (as Canadians have been able to do for years) and can request credit watches, or freezes, to be applied to their reports. As individuals are notified of security breaches involving their personal information, they will have the opportunity to access and view their entire record and any disclosures made for accuracy or lack thereof; they will also be able to request that changes, corrections, and deletions be made to their files.

The current legislative interest on behalf of the rights of the individual stems from fundamental data privacy practices expressed in the early 1970s by the U.S. Department of Health and Welfare, e.g.:

- provide data subjects with information about their data activities;
- obtain any form of consent for processing of personal data;
- permit opt-out of processing by data brokers;
- offer rights of access or correction; and
- assume liability for errors that harm individuals.

As expressed in these Fair Information Practices, an individual's interests are advanced by the following principles:

> **Consent** – *The knowledge and consent of the individual are required for the collection, use or disclosure of personal information, except when inappropriate.*

Most data privacy laws revolve around the concept of individual consent. This principle brings the individual directly into the picture by vesting him or her with certain participatory rights in the information and how it is managed.

Consent can take a wide variety of forms depending on the circumstances but in general, and as a best practice, consent should be fully *informed* and *explicit*. It will increasingly be unacceptable for organizations to ask people to consent to something that they know nothing about or understand.

In many cases, the consent principle also imposes a duty upon organizations that collect personal information to record consent preferences and to ensure that these preferences are honoured, especially when sharing data with third parties.

An important aspect of consent is that it may be revoked or withdrawn by the individual. Consent that cannot be revoked typically has less validity. Withdrawn consent often imposes an obligation on an organization to ensure that other organizations with whom it has shared that data also honour the revocation.

Firms that do not have processes in place for recording consent and for honouring requests for withdrawal (i.e., take me off your mailing list), will have to face the consequences.

Witness the recent decision of the Federal Privacy Commissioner regarding a major bank's practice not to do so.[50]

> **Accuracy** – *Personal information shall be as accurate, complete, and up-to-date as is necessary for the purposes for which it is to be used.*

It is a long-established principle that individuals are entitled to expect that decisions made about them will be based upon accurate information and that, moreover, they are entitled to know about and inspect any files held about them in order to verify accuracy and request corrections, if necessary.

By the same token, organizations are obliged to ensure the accuracy of the personal data they hold and use for decision-making purposes. Some do this by encouraging and making it easy for their customers to access and amend their own information, such as accessing their "profiles" and preferences. Other firms maintain accuracy by routinely discarding personal records upon a pre-set expiry date.

As the old saying goes, "Garbage in. Garbage out." Inaccurate or out-dated information can result in correspondingly bad decisions. And if those decisions are automated and materially impact the individual — such as their ability to obtain employment, a promotion, credit, insurance, reasonable accommodations, travel, etc. — then there may be a basis for a complaint and remedial action. A significant percentage of data compiled on all of us, held in dossiers, and sold to businesses and governments by infomediary brokers and data aggregators, is inaccurate.[51] In a recent study, the U.S. Public Interest Research Group found that one in four credit reports contained serious errors.[52]

> **Openness** – *An organization shall make readily available to individuals, specific information about its policies and practices relating to the management of personal information.*

Individuals (not to mention business partners and affiliates carrying out due diligence activities, as well as regulators and other oversight bodies), cannot evaluate the privacy and security claims of organizations to assess their trustworthiness without some degree of openness. Sunshine is the best disinfectant, especially where there is cause for concern.

> **Access** – *Upon request, an individual shall be informed of the existence, use and disclosure of his or her personal information and shall be given access to that information. An individual shall be able to challenge the accuracy and completeness of the information and have it amended as appropriate.*

50 Privacy Commissioner of Canada, PIPEDA Case Summary #308: Opting-out of marketing inserts in account statement at **www.privcom.gc.ca/cf-dc/2005/308_20050407_e.asp**. Coverage at **www.michaelgeist.ca/index.php?option=content&task=view&id=907**.

51 See, for example, the May 2005 survey at **www.privacyactivism.org/docs/DataAggregatorsStudy.pdf**.

52 **http://uspirg.org/uspirgnewsroom.asp?id2=13650&id3=USPIRGnewsroom&**.

The principle of "no secret dossiers" has typically accompanied the individual's right to access, inspect and, where possible, request amendments, corrections, or annotations to any files held on him or her. Access to credit reports has become a well-established privacy right in Canada and the United States that also applies to files detailing medical records or payments, residential or tenant history, cheque writing history, employment history, and insurance claims.

As more organizations compile ever-larger records on individuals, and as the negative implications and uses of those files become more evident, there is every reason to believe that the access principle will be expanded to more and more domains.[53]

When revelations of the Canadian Human Resources Development Agency's "Longitudinal Database" became known to the public, containing as many as 2000 data items on millions of individual Canadians, the agency received over 75,000 access requests in one month before dismantling the entire database.[54]

Firms are well-advised to have systems in place that allow them to respond to access requests in a timely manner.

> **Challenging Compliance** – *An individual shall be able to address a challenge concerning compliance with the above principles to the designated individual, or individuals for the organization's compliance.*

When misunderstandings, disagreements, and disputes arise, it is best for all parties to have established escalation and mediation procedures in place. In Canada, Privacy Commissioners and the courts serve in many instances as the forums for investigating and resolving disputes.

From the perspective of the individual, the availability of avenues of redress that include the possibility of adverse decisions, negative publicity, restoration of damages, fines, and other binding consequences on the organization in question can serve to strengthen the negotiation and ensure that the individual's concerns are addressed as early as possible.

Privacy is *Comprehensive*: Privacy Enhances Security

> **Safeguards** – *Personal information shall be protected by security safeguards appropriate to the sensitivity of the information. Safeguards must be assured through reasonable physical, operational, and electronic means.*

Typically, privacy principles and laws do not provide much detail or guidance on security, leaving it up to organizations to decide what constitutes "appropriate" and "reasonable" security measures.

53 See FTC report on online access available at **www.ftc.gov/acoas/**.

54 The number of Privacy Act requests received by HRDC as a result of the May 2000 news story jumped from 8,443 in Fiscal Year 2000 (which ended on April 30, 2000) to 75,669 in Fiscal Year 2001 (Treasury Board Secretariat 2000, InfoSource Bulletin Number 23. Ottawa: November 2000 p. 14; Treasury Board Secretariat, Ottawa: August 2001, InfoSource Bulletin Number 24: p. 13).

While the IT community has the necessary expertise to define what reasonable security looks like, IT professionals still face the greater challenge of how to persuade the rest of the company to adhere to reasonable security standards. Many of the privacy-breach incidents that have appeared in the headlines this year demonstrate a failure of business practices, not a failure of information technology.

Many of the security breaches identified may have been avoided if simple physical safeguards had been in place and adhered to: computer databases that were physically lost or stolen in transit, hard drives physically removed from computers, laptops gone missing from sidewalks, taxicabs, hotel rooms. In many instances, physical access to the data or media is all that is needed for a privacy breach to take place.

Similarly, the growing recognition of the ability of insiders to quickly attach peripheral memory and storage devices to computers to effortlessly copy large volumes of sensitive data is being met by new techniques and technologies that physically prevent this from happening. It's harder to steal the data if your USB memory stick won't connect, or there is literally no place to insert a floppy.

While physical security measures are important, they must increasingly be supported in depth by organizational and technological reinforcements. Below is a sampling of proven technological means of safeguarding data from unauthorized access and use. While these methods may not entirely eliminate the problem, they will surely lead to a significant reduction.

Database Encryption

After limiting physical access, the single most important action is to secure data by encrypting it, not just in transit, but also in its place of storage. That way, when the hard drive or laptop is physically stolen, or when the data is copied, the personal information stored on it cannot be accessed, read or used. If the data is encrypted, the need to report it as lost or stolen and to notify the subjects also becomes less urgent.

While this may seem somewhat surprising, most databases, even the high-end sophisticated ones, continue to store data in clear text format (unencrypted), and even more surprising, those large data stores are routinely transferred, synchronized and backed up using unencrypted, insecure transmission methods and media.[55] So why should it come as a surprise that personal data is routinely stolen and identity theft is on the rise? Yet intelligent, cost-effective information technologies that automatically encrypt critical data wherever they are stored across an enterprise — in applications,

55 Only 7% of businesses encrypt all backup tapes, and even fewer encrypt data at the application or database layer, according to a March 2005 research report by Jon Oltsik and John McKnight at Enterprise Strategy Group, *Information at Risk: The State of Backup Encryption* available at **www.enterprisestrategygroup.com/_documents/Report/Attachment2ID393.pdf**.

Cited May 4 2005 in "After Data Losses Like Time Warner's, Companies Need To Rethink Tape-Storage Security," *InformationWeek* at **www.informationweek.com/shared/printableArticle.jhtml?articleID=162101437**.

databases or backup tapes— exist today and are widely available, such as I.B.M.'s new x9 mainframe[56] and solutions from Ingrian DataSecure.[57]

Severing or Encrypting Personal Identifiers

Another proven approach is to encrypt or replace certain sensitive database fields, or to otherwise sever the personal identifiers from the data record itself. This may be achieved through the use of a link or pointer to the personal identifiers as is often done in health care establishments with patient records, so that the data, in effect, becomes anonymized. When AOL's entire customer database was stolen in 2003, containing millions of records, customers' real names and other personally identifiable information were not included because a "severance function" had been activated.[58] Standardized and hashed identifiers could be used to carry out privacy-enhanced data matches and checks without exposing any personally identifiable information. This is the core idea behind I.B.M.'s new suite of information management tools, called DB2 Anonymous Resolution.[59]

Data Aggregation, Perturbation and Anonymization

Other privacy approaches seek to manipulate the data in such a way that individually identifiable records cannot be retained. Aggregation, statistical perturbation, and other data anonymization techniques are important privacy-enhancing processes. Such techniques effectively strip away key identifiers and, with them, the ability of data recipients to be able to match and re-identify individual records. Such techniques allow the routine disclosure and active dissemination of data contained in forms, and for some purposes that are effective and statistically valid, but simply not identifiable to an individual.

Data Item Masking

The next best solution is to mask the sensitive elements of database records from being accessed, transmitted, displayed, printed or otherwise disclosed or modified. The personal information stays in the database record but is not accessible without proper authorization. For example, it may not be necessary for a customer service representative to see a customer's entire record. Nor should a customer's entire credit card number be printed on the sales receipt – four digits will suffice, with the remainder being masked. This is commonly referred to as "truncating" a number of the digits of one's credit card number.

56 See "I.B.M. Introduces New Line of Mainframe Computers", reported in The New York Times, July 17, 2005 at **www.nytimes.com/2005/07/27/technology/26cnd-ibm.html**?

57 Ingrian DataSecure Solutions at **www.ingrian.com/products/** and **www.ingrian.com/news/pr050627.html**.

58 However, 92 million AOL usernames and email addresses were stolen and used illegally to send billions of spam messages. For news coverage, see **www.nytimes.com/2005/02/05/technology/05spam.html** and/or **www.washingtonpost.com/wp-dyn/articles/A860-2004Jun23.html**.

59 I.B.M.'s DB2 Anonymous Resolution information at: www-306.ibm.com/software/data/db2/eas/anonymous/This concept and similar applications are discussed at some length in the April 2002 book *Translucent Databases* by Peter Wayner. (ISBN 0967584418). An excellent overview and discussion by Simson Garfinkel of hash functions is available at: **www.techreview.com/articles/04/08/wo_garfinkel080404.asp**.

Identity Management/Access Controls

Another solution is to set rigorous access controls on the database and its contents. Innovative new approaches are being tried in this area, notably by adding "metadata" to records and data items that can specify purposes, preferences and other conditions of use. Access controls, and other usage policies, can then be automatically enforced through the use of automated mechanisms that read and apply the metadata, such as:

- Role-based "need-to-know" use;
- Identity management and provisioning;
- Use of 2- and 3-factor authentication;
- Authorization.

It is common for organizations to fail in revoking access on a timely basis, so that former employees, including contractors and temporary employees, may still maintain their network credentials, (e.g., passwords), for a considerable amount of time after they have left the organization.

Effective access controls require good enterprise-wide identity management techniques. When an employee leaves an organization, their username, password, and other network access and authorization privileges should all be revoked at the very time of departure. There is no excuse for a delay in this action since it should be a simple and quick task to perform. The average company has more than 100 directories in which identity information is stored. I.B.M. estimates up to 60% of company access profiles are orphaned accounts (e.g., employees who have left the company or changed jobs) creating serious security gaps.

According to highly acclaimed U.S. security expert Bruce Schneier, "Identity management systems are critical for organization. But they're less about security and more about process efficiency. When someone moves around in an organization – gets hired, fired, promoted or goes on vacation – their access to resources changes. Identity management systems allow administrators to deal with their information accesses in one easy place."

It appears that Enterprise Identity Management Systems are now in great demand, with many products and systems available. For a comprehensive overview and authoritative study of identity management systems from a privacy point of view, see the comprehensive report from the EU Privacy and Identity Management in Europe (PRIME), entitled *Identity Management Systems* (IMS): *Identification and Comparison Study*.[60]

60 Independent Centre for Privacy Protection (ICPP), *Identity Management Systems (IMS): Identification and Comparison Study* (September 2003), available at: **www.datenschutzzentrum.de/download/IMS/IMS-Study-final.pdf**.

The Inside Job

Apart from human error and hacker threats, inside theft is a big problem. It is well known that insiders who access databases often have network authorization, knowledge of data access codes and a precise idea of the information they want to exploit.

Further, there are more unauthorized accesses to databases than corporations admit to their clients, stockholders or business partners. Gartner Group estimates that internal employees commit 70% of information intrusions, and more than 95% of intrusions that result in significant financial losses. A 2002 survey of 163 *Fortune* 1000 companies found that 70% of reported security breaches were linked to insiders.[61]

Another survey by the Computer Security Institute revealed that over half of all corporate databases had some kind of breach every year, with the average breach resulting in close to $4 million in losses.[63] And these are only the security breaches that are reported.

There is no magic bullet solution to the insider abuse of personal information. At some point, employees must be allowed a certain measure of trust and latitude to go about their jobs. However, a variety of new technologies and techniques are emerging that can help establish automatic and enforceable boundaries around data access, use and sharing, followed by the use of audit trails to detect fraudulent activity, after-the-fact.

Chief among these are technologies that impose strict network and database access controls. When supported by automated logging and audit trails, strong access controls can go some way to reducing abuse of data. Increasingly, organizations are "locking down" data from unauthorized copying by preventing peripheral memory devices, such as floppy disks and USB sticks, from connecting to computers and saving data. Hard drives that self-destruct or "phone home" when removed from their proper environment are examples of technologies that can deter insider theft.

Similarly, new technologies allow finer restrictions on staff ability to print or forward sensitive messages or personal data. Sophisticated network filtering devices are now being developed and deployed that can detect when sensitive information is being sent out through the network, for example, by email or email attachment, in a manner analogous to scanning incoming messages and attachments for viruses or inappropriate content.

61 Mogul, Richard, "Danger Within – Protecting your Company from Internal Security Attacks," *CSO Online*, August 21, 2002, **http://www.csoonline.com/analyst/report400.html**.

62 Computer Security Institute/FBI Computer Crime and Security Survey, 2002.

63 For details, see **www.realuser.com**, **www.realuser.com/news/pdf/Pictures%20as%20passwords%20-%20Economist.pdf** , **http://csrc.nist.gov/pki/twg/y2003/papers/twg-03-11.pdf** and **www.mddailyrecord.com/guestbook/realuser.html**.

Strong Authentication

Strong, reliable methods of authentication are necessary to ensure that only authorized individuals, both internal and external, can access and use the data. Many security breaches are the result of poor access control procedures and technologies, by both staff and clients.

Some typical authentication remedies are:

- Better password management and protection;
- Innovative use of new reminder phrases and password substitutes, such as "Passfaces;"[62]
- Increasing use of two- and even three-factor authentication, e.g., secure ID tokens, RFID-enabled "proximity" access cards, and biometrics; and
- Avoid using identification or passwords that are the default, easily guessed or accessible, e.g., social insurance/security number or mother's maiden name.

Equifax Canada, a large credit reporting agency, has deployed a system of authenticating the identities of individuals who request copies of their credit report by asking them a series of "out-of-wallet" questions derived from their credit histories, such that they and only they, would know the answers. So, for instance, you might be asked (among other questions) whether or not you have had a car loan, the amount of your monthly payments, and with whom the loan was held.[64]

Digital Rights Management (DRM)

DRM technologies also offer innovative approaches to managing and controlling sensitive information within a given work context or environment. These technologies can enforce fine-tuned controls over the use and disclosure of data by others, such as their ability to view, copy, print, or forward. DRMs can even auto-delete data or messages not required beyond a specified time period. In the event that data is leaked or exposed, DRM may also make it possible to track and trace the data itself.

Audit Trails / Electronic Tracking

A key issue to consider when purchasing a database security solution is making sure you have a secure electronic audit trail for tracking and reporting activity regarding confidential data, such as personal information.

Information systems and processes should be designed from the start to minimize the collection, use and disclosure of personal data.[65] Additional levels of checks and authorizations should also be employed to access higher levels of sensitive data. Default settings should always be set to "no access" unless authorized, rather than the opposite.

64 See **www.equifax.com/EFX_Canada/services_and_solutions/ecommerce_solutions/eidsol_e.html**.

65 See Ann Cavoukian, Ph.D., Information and Privacy Commissioner/Ontario, Security Technologies Enabling Privacy (STEPs): Time for a Paradigm Shift (June 2002) available at: **www.ipc.on.ca/docs/steps.pdf**.

A record of all databases accessed should be kept to help detect, deter, and if necessary, prosecute misuse and abuse after the fact. Clear organizational policies should guide the use of these logs.

Network logging and monitoring can also serve as an important deterrent and enforcement tool. It should be carried out automatically, routinely, quietly, accurately, and without human intervention. For example, intrusion detection systems attempt to monitor database and network usage for anomalous behaviour, such as repeated log-in attempts or large file transfers.

Independent third party audit, attestation, and certification may also be desirable for some companies to credibly demonstrate compliance and earn greater trust, especially with downstream and upstream suppliers, and other business Web partners.

With regard to the privacy and security of customer data, all forward transfers and use of customer data with affiliates and partners should be assured by contract and other legal mechanisms. 80% of firms fail to conduct a regular assessment of their IT outsourcer's compliance with the host organization's information security requirements. Moreover, 70% fail to conduct a regular assessment of their IT outsourcer's compliance with the host organization's information security policies.[66]

Building a Culture of Privacy

The majority of the recent security breaches may not have taken place if there had been formal organizational mechanisms in place. For example, if fax numbers had been double-checked after complaints of misdirected faxes, or if client credentials had been verified prior to giving access to databases of personal information. Most important, there should always be a chain of command in place, consisting of individuals whose duties include dealing with security and privacy breaches.

Moreover, recklessness or simple carelessness of a single employee can undermine even the best technological countermeasures. Many security breaches are simply the result of human error, enabled by weak operational practices. For this reason, attackers will invariably focus on the weaknesses of people and processes — the weakest link.

A marginal number of companies have instituted comprehensive internal training and awareness programs for their employees to learn about privacy and security. New technologies also offer unparalleled opportunities to inform staff about company policies, their responsibilities, and how to meet privacy and security obligations.

Lack of Awareness: Conventional wisdom says that most individuals are simply not aware of the importance of security measures as they go about their daily routines. Heightening the awareness of all employees can go a long way.

66 Global Information Security Survey 2004, Ernst & Young, page 21.

Crisis Management

Although many organizations have a business continuity plan, surveys suggest that few have adequately been tested, and that most contingency plans never survive past the point of first contact with the reality of a privacy or security breach. A 2005 Ponemon Institute survey of corporate privacy practices found that only a third of companies use a formal process to monitor and report security breaches.[67]

In our view, all organizations should implement a Privacy Crisis Management Protocol immediately upon learning of the breach. The five steps of such a protocol consist of:

1 **Containment:** Identify the scope of the potential breach and take immediate steps to contain it: retrieve the hard copies of any personal information that has been disclosed; ensure that no copies of the personal information have been made or retained by the individual who was not authorized to receive the information and obtain the individual's contact information in the event that follow-up is required; and determine whether the breach would allow unauthorized access to any other personal information (e.g., an electronic information system) and take whatever steps are appropriate (e.g., change passwords and/or temporarily shut down a system).

2 **Notification:** Identify those individuals whose privacy was breached and, barring exceptional circumstances, notify those individuals accordingly: notify the individuals whose privacy was breached, by telephone or in writing; provide details of the extent of the breach and the specifics of the personal information at issue; and advise of the steps that have been taken to address the breach, both immediate and long-term.

3 **Communication:** Ensure appropriate staff within your organization are immediately notified of the breach; advise the Privacy Commissioner and other relevant oversight agencies of the breach and work together constructively with their staff.

4 **Investigation:** Conduct an internal investigation into the matter, linked to any external investigation. The objectives of the investigation are to: 1) ensure the immediate requirements of containment and notification have been addressed; 2) examine the circumstances surrounding the breach and determine what caused it; and 3) review the adequacy of existing policies and procedures to protect personal information.

5 **Improving Practices:** Address the situation on a systematic basis. In some cases, program-wide or institution-wide procedures may warrant review; in other situations, compensatory action or other forms of restitution for affected individuals may be warranted.

67 Cited in Ponemon, Larry, "Opinion: After a privacy breach, how should you break the news?" (July 5, 2005) in ComputerWorld at **www.computerworld.com/securitytopics/security/privacy/story/0,10801,102964,00.html**.

Consumer Self-Help Tips

While we have stated that consumers are not responsible for the large-scale occurrences of identity theft emanating from poor data management practices, there are nonetheless steps that can be taken to attempt to minimize the risk of becoming a victim of identity theft:

1 Minimize the amount of personal information you give out, especially online;

2 Do not give out your SSN/SIN, unless absolutely necessary; never disclose it online; never use it as a password;

3 Keep items containing personal information, such as your birth certificate, passport, citizenship card, etc., in a safe place;

4 Guard your mail from theft; add a lock to your mailbox;

5 Pay attention to your billing cycles; carefully review bills and statements on a regular basis; monitor your account balances and activity frequently;

6 Obtain and review your full credit report every year; mark the date in your calendar as a reminder;

7 Notify creditors immediately if your cards are lost or stolen;

8 Obtain a separate credit card dedicated to the exclusive use of your online purchases (with the lowest credit limit possible);

9 Shred all personal records and financial statements instead of just throwing them into the wastebasket;

10 Beware of dumpster divers: ask businesses that you deal with (like car rental agencies) to shred your application forms upon completion of their use;

11 Ask companies who print your entire credit card number on the sales receipt to consider truncating the number (so it doesn't appear in its entirety); and

12 Be very wary of responding directly online to any e-mail request for personal information sent by online service providers (phishing), or an alleged superior within your organization (spear-phishing). Instead, contact the institution or sender through another communication channel – call them by phone, using a pre-existing number.

If you have already become a victim:

1 Immediately report the crime to the police; keep a copy of the occurrence report;

2 Armed with the police occurrence report, advise all businesses with whom you have a relationship of the possible loss, theft, or misuse of your identity. Ask for stronger security measures — have a fraud alert placed on your accounts; start with the credit bureaus;

3 Cancel all your cards and accounts, and open new ones;

4 Document all the steps you have taken and your expenses to clear your name and re-establish your credit;

5 Have your credit reports annotated or possibly "frozen;"

6 Contact the Post Office if you suspect that someone is diverting your mail – beware of false change of address forms; and

7 Consider telling your employer, as an added precaution.

Summary / Conclusions

Privacy is Good for Business: A growing body of evidence indicates that organizations that adopt open and effective information management practices, which respect their customers' personal information, are benefiting in many ways.

The outbreak of recent high-profile data security breaches in 2005 has had the unintended benefit of exposing long-term problems in the way that organizations have been managing sensitive customer data. Consequently, this has drawn the attention and critical scrutiny of the public, shareholders, and lawmakers. In response, a wide range of legislative responses are being proposed based on growing support for the early notification of data security breaches, and for imposing some measure of liability on firms who mismanage customer data.

It is becoming recognized that the single largest cause of identity theft derives from poor information management practices. There is a growing belief that organizations that collect, use and share personal information should bear greater responsibility for their actions, especially in the case of negligence that negatively impacts consumers and the public. Preventative measures must be taken at the outset to ensure that customer data is strongly protected.

This is a critical time for businesses — to take the opportunity to review and improve their information management policies and practices. This is clearly necessary not only to avoid negative publicity and litigation, but also to build enduring trust with customers, partners and stockholders. Towards this end, businesses should consider the fundamental insights that data privacy can offer to organizational security, namely:

1 **Data Privacy is Comprehensive** – it applies not only to the data itself but to the entire environment in which that data is collected and used;

2 **Data Privacy is Personal** – the interests of the data subject must be considered and built into information systems and controls; and

3 **Data Privacy Enhances Security** – by minimizing collection, use, disclosure and retention of sensitive personal data, privacy-enhancing technologies can contribute to stronger data security.

In summary, a proactive approach to data privacy and security will position an organization as a leader, differentiate it from the rest of the pack, and pay handsome dividends in terms of reduced costs associated with crisis management and damage control. Most important, it will lead to improved customer trust, goodwill, and loyalty. Too many businesses avoid taking an "outlier" approach to data privacy and security: the tendency is to keep one's head down, stay in the middle of the pack, and try not to get too far in front (or behind) the others, for fear of being singled out for attention. We think you should do the opposite.

Over time, this will prove to be a poor business strategy, as privacy and security incidents will invariably occur. However, the most proactive, open and accountable firms will suffer the least from the fallout. A proactive approach will provide an important head start on the coming wave of privacy legislative and regulatory measures being proposed and adopted across the United States and in Canada. Our advice — get in front of the crowd, develop strong information management practices, encrypt personal information holdings, and reap the benefits.

Incorporating Privacy into Marketing and CRM

May 2004

Introduction

With sales of more than $13.3 billion worldwide in 2003, Eastman Kodak's products and services reach millions of customers around the world.[1] As with many companies, Kodak engages in customer relationship management (CRM), a business strategy which focuses on developing a better understanding of the needs and preferences of customers so that a company can strengthen its relationships with its customers. But Kodak is going one step further – it is actively integrating privacy principles into its global CRM strategies, particularly with respect to marketing.

In 2001, Kodak's newly appointed chief privacy officer, Dale Skivington, approached the company's chief marketing officer and proposed that an internal privacy council be established that would take an internationally recognized set of privacy principles, known as fair information practices, and apply them to the marketing activities of all of Kodak's business units around the world, including those in Canada. After the council was established, it developed privacy guidelines for each type of marketing activity and the company began investing in CRM technology that complemented Kodak's emphasis on privacy.[2]

Businesses are increasingly recognizing that privacy can play a crucial role in the success of CRM initiatives. A 2002 study, by the U.S.-based Gartner research group, found that 40 per cent of companies were rethinking their CRM projects to include a greater emphasis on privacy.[3] In Canada, the extension of privacy legislation to the private sector is also influencing the implementation of CRM. As of January 1, 2004, the federal *Personal Information Protection and Electronic Documents Act* covers all private-sector organizations that collect, use or disclose personal information in the course of commercial activities, except in those provinces that have enacted substantially similar legislation.[4]

The challenge for businesses implementing CRM is to collect, use and disclose personal information in a manner that does not invade the privacy of their customers. Although CRM is used for a wide variety of purposes, the vast majority of Canadian companies use CRM for marketing purposes. In this paper, we will argue that building a privacy framework into CRM initiatives is not only a legal necessity in Canada but can play a pivotal role in maintaining customer trust and loyalty, which is the ultimate goal of CRM. In particular, we will outline some practical steps that businesses can take to integrate fair information practices into their CRM projects, particularly those that involve marketing.

1 Eastman Kodak Company, News Release, "Kodak Has 4th-Quarter Reported Net Income of 7 Cents Per Share," January 22, 2004, <**www.kodak.com/US/en/corp/pressReleases/pr20040122-05.shtml**>.

2 Telephone interview with Dale Skivington, March 1, 2004.

3 "Report: Companies Must Balance Privacy with CRM Programs," *DM Review*, January 2002, <**www.dmreview.com/editorial/dmreview/print_action.cfm?articleId=4595**>.

4 S.C. 2000, c. 5, <**www.privcom.gc.ca/legislation/02_06_01_e.asp**>. Please recognize that this document does not offer legal advice nor does it intend to provide an interpretation of the *Personal Information Protection and Electronic Documents Act* (PIPEDA). It does provide best practices for your organization to consider in its administration of PIPEDA. Please consult your own legal advisors on steps your organization may need to take to ensure compliance with PIPEDA.

CRM and Canadian Businesses

Although there is little agreement on how to define CRM, it generally covers a range of activities used by businesses to gain insight into customer needs and behaviours in order to strengthen their relationships with their customers. In its "pure" form, CRM allows businesses to better understand the individual needs and preferences of their key customer segments, and to serve different customers differently.[5] CRM encompasses strategies and technologies that are enabling companies to move from product-centric business models to ones that are customer-centric.

A CRM benchmark study, published by the Canadian Marketing Association (CMA) in 2002, found that 86 per cent of Canadian companies in nine sectors of the economy practised some form of CRM.[6] Although the study found that CRM is still developing in Canada, it noted that CRM expenditures were projected to top $800 million in 2003 and climb at a compound annual growth rate of 15 per cent.[7] In short, CRM is rapidly becoming entrenched as an established business practice in the Canadian marketplace.

What is Privacy?

In North America, the legal concept of privacy was first explored in an 1890 article in the *Harvard Law Review* by Professors Samuel Warren and Louis Brandeis who defined privacy as "the right to be let alone."[8] This definition of privacy has evolved over the last century to include at least two strands: the right of individuals to control their physical space (i.e., their body or home) and to control their personal information. The latter right is known as "informational privacy" or data protection.

Consequently, privacy includes the right of individuals to control the collection, use and disclosure of personal information about themselves. Personal information can be defined generally as identifiable information about an individual. In other words, it is information that serves to identify a person and could include his or her name, address, telephone number, date of birth, age, marital or family status, financial status, e-mail address, etc.

Private-Sector Privacy Legislation in Canada

The federal government enacted the *Personal Information Protection and Electronic Documents Act* (PIPEDA) to protect personal information that is collected, used and disclosed by private- sector organizations in the course of commercial activities. The legislation has come into effect on a staggered basis. On January 1, 2001, PIPEDA applied to federally-regulated businesses such as banks, railways, airlines and broadcasting companies. On January 1, 2004, the legislation further extended to provincially

5 Canadian Marketing Association (CMA), "CRM Benchmarks: Canada 2002 Edition – A Roadmap for Improving Customer Relationships," p. 7. The CMA, the Carlson Marketing Group and The Loyalty Group jointly sponsored the study. Decima Research Inc. conducted the study in partnership with Deloitte Consulting. To order the study, go to: <**https://www.the-cma.org/forms/crmbenchmarks_form1.html**>.

6 Ibid., pp. 11, 17.

7 Ibid., p. 7.

8 <**www.louisville.edu/library/law/brandeis/privacy.html**>.

regulated businesses, unless a province had enacted substantially similar privacy legislation. Quebec has had private-sector privacy legislation in place since 1994.[9] British Columbia[10] and Alberta[11] brought in their own private-sector privacy legislation on January 1, 2004. However, businesses in other provinces, such as Ontario, are subject to PIPEDA.

What are Fair Information Practices?

Canada's privacy laws are based on fair information practices which are a set of common standards that balance an individual's right to privacy with an organization's legitimate need to collect, use and disclose personal information. In 1980, fair information practices were internationally codified in the Organisation for Economic Co-operation and Development's *Guidelines on the Protection of Privacy and Transborder Flows of Personal Data*.[12] In 1996, these standards were incorporated into the Canadian Standard Association's *Model Code for the Protection of Personal Information* (CSA Model Code).[13] The CSA Model Code, which is appended as a schedule to PIPEDA, includes the following 10 fair information practices:

- Accountability
- Identifying Purposes
- Consent
- Limiting Collection
- Limiting Use, Disclosure, and Retention
- Accuracy
- Safeguards
- Openness
- Individual Access
- Challenging Compliance

9 *An Act Respecting the Protection of Personal Information in the Private Sector,* R.S.Q. c. P-39.1, <**http://publicationsduquebec.gouv.qc.ca/dynamicSearch/telecharge.php?type=2& file=/P_39_1/P39_1_A.html**>.

10 Bill 38, *Personal Information Protection Act*, 4th Sess., 37th Parl., British Columbia, 2003 (came into force on January 1, 2004), <**www.legis.gov.bc.ca/37th4th/3rd_read/gov38-3.htm**>.

11 *Personal Information Protection Act*, S.A. 2003, c. P-6.5, <**www.qp.gov.ab.ca/documents/acts/p06p5.cfm?frm_isbn=0779725816**>.

12 <**www1.oecd.org/publications/e-book/9302011e.pdf**>.

13 <**www.csa.ca/standards/privacy/code/default.asp?language=english**>.

Applying Fair Information Practices to CRM

CRM initiatives involve the collection, use and disclosure of personal information, particularly for marketing purposes. Since understanding customers is critical to building relationships, businesses implementing CRM may collect information about who their customers are, what they purchase, their satisfaction levels and their channel preferences. Individuals interact with businesses through a variety of channels – stores, call centers, websites, e-mail campaigns, telemarketing, direct mail campaigns and sales people in the field. Although only half of Canadian companies can currently integrate customer data across service channels,[14] the promise of CRM is that the more holistically a company can view information from disparate sources, the more it can tailor products and services to fulfill customers' wants, needs and preferences. As CRM sophistication increases, so does the need to implement appropriate safeguards for personal information and to abide by customers' privacy expectations.

To comply with the requirements of privacy legislation and to avoid alienating customers, businesses must find ways to incorporate fair information practices into CRM initiatives. However, since CRM includes a loosely defined range of activities that could change over time, incorporating fair information practices into CRM may not always be straightforward. Consequently, the actions taken to protect privacy may vary depending on the size of the business, the resources that are available for this purpose, the extent to which CRM has been incorporated into a company's business strategies, and the amount and sensitivity of the personal information that is collected, used and disclosed for the purposes of CRM.

FIP #1: Accountability

An organization is responsible for personal information under its control and shall designate an individual or individuals who are accountable for the organization's compliance with the following principles.

Many individuals within a business, such as sales, marketing or website staff, may be responsible for the day-to-day collection and processing of personal information for the purposes of CRM. However, a business must designate one or more specific individuals who are accountable for ensuring that the business complies with fair information practices and privacy legislation. In large companies, a chief privacy officer would typically play such a role. In medium and small companies, such a role could be fulfilled by a privacy officer or another designated staff person who is properly trained in privacy management.

As a best practice, the designated individual should be actively engaged in the design and implementation of CRM initiatives to ensure that fair information practices are taken into consideration. For example, as noted previously, Kodak's chief privacy officer approached the company's chief marketing officer shortly after she was appointed in 2001 and proposed that an internal privacy council be established that would apply fair information practices to the marketing activities of all of Kodak's business units around the world.

14. Supra note 5, p. 51.

It should also be noted that a business is responsible for personal information that is in its possession or custody, including information that has been transferred or outsourced to a third party for processing. Consequently, if a company hires an external CRM consultant to perform data analysis or a variable printing supplier to execute a mailing, it must ensure that these outside entities are contractually bound to provide a comparable level of privacy protection to this data.

Finally, a business must put into place policies and practices that give effect to the 10 fair information practices, including:

- implementing procedures to protect personal information;
- establishing procedures to receive and respond to complaints and inquiries from the public;
- training staff and communicating information to staff about the business' policies and practices; and
- developing information to explain the business' policies and procedures.

FIP #2: Identifying Purposes

The purposes for which personal information is collected shall be identified by the organization at or before the time the information is collected.

According to the CMA's 2002 benchmark study on CRM, 90 per cent of companies collect basic "tombstone" information about their customers (e.g., name, address), purchase history, customer satisfaction information, and data on customer loyalty and retention.[15] More than 75 per cent of businesses also gather customers' opinions about their products, services and the overall industry.[16] Seventy per cent of companies collect demographic information about customers, such as their household income and age.[17]

Companies collect this information for a variety of CRM-related purposes. In general, it is collected for the purpose of better understanding and serving the needs and preferences of customers. However, there is a requirement that information must be gathered for specific, identified purposes. Companies must not solicit or collect information on an ad hoc basis or engage in "fishing expeditions" to accumulate personal information for some vague potential future use. Companies must articulate how they intend to use the information (e.g., for marketing purposes, for customer service, to administer a loyalty program, for credit verification, etc.) and collect only the information that is necessary for the identified purposes.

As a best practice, businesses should err on the side of transparency and be as open as possible when identifying the purposes for which they are collecting personal information from their customers.

15. Ibid., p. 41.
16. Ibid.
17. Ibid.

Consumers may be informed about the purpose for which information is being collected in a variety of ways, depending on the communication channel. For example, if a consumer buys a product from a company's website and is asked to provide demographic information such as annual income and age, a privacy policy that identifies the purposes for the collection should be easily accessible on the website. In face-to-face or in-store interactions, it may be more practical to provide written policies or have staff trained so they can accurately answer questions from their customers.

When personal information that has been collected is to be used for a purpose that was not previously identified, the new purpose must be identified prior to its use. For instance, a hardware company may have initially collected the names and addresses of customers from filled-in ballot forms for the purpose of administering a contest. The company would have their customers' implied consent to use their information to inform them whether or not they had won the contest. However, if the company later wishes to use this contest information for other purposes, such a direct mail campaign for do-it-yourself products, it must obtain consent and provide an opportunity to decline from receiving marketing offers.

FIP #3: Consent

The knowledge and consent of the individual are required for the collection, use or disclosure of personal information, except when inappropriate.

Businesses must seek permission from customers before collecting, using and disclosing their personal information for CRM-related purposes, such as presenting new marketing offers or renting a customer list to other companies. Customers must have the opportunity to provide informed consent, which means that they understand the nature and consequences of providing or withholding consent. In a multi-channel CRM environment, it is recognized that there are several appropriate methods of obtaining consent to conform to fair information practices and to build trust between companies and their customers. The law also takes a common sense approach to the sensitivity of the information being collected, used or disclosed.

Consent is commensurate with the sensitivity of the data. For less sensitive information, such as a customer's name, address or telephone number, it is appropriate for a company to seek opt-out consent. In other words, unless a customer opts out, a company would be allowed to use or disclose that individual's name, address or telephone number for the purpose of marketing new products or services to that customer. However, the opt-out consent must be clear, easy to understand and easy to execute. (A best practice may include offering a toll-free number to opt out.)

In some circumstances, where the marketing offer is intimately linked to an original transaction, companies may reasonably conclude that consent is implied and does not need to be specifically requested. For example, a magazine publisher would have a subscriber's implied consent to send out subscription renewals. However, the disclosure of personal information to a third party for marketing purposes can never be implied – it must be obtained by opt-out or opt-in consent.

If a company is collecting sensitive information from customers, such as their personal health information or financial information, it must not use or disclose this information for marketing purposes unless the individual has opted in (i.e., provided express, explicit consent). Beyond obviously sensitive information – medical, credit, financial, sexual orientation, etc. – companies should give serious consideration to how a consumer may regard other types of information prior to using it (e.g., certain magazine subscriptions).

Companies can allow customers to give consent in many ways – by mail, phone, online, in store or through any appropriate channels. Current best practices in Canada can be found in the privacy policies and practices of leading CRM companies. Examples include Hudson's Bay Company – hbc.com, Kodak Canada – kodak.ca, The Loyalty Group – airmiles.ca, RBC Financial Group – rbc.com and Reader's Digest – readersdigest.ca

Companies collecting personal information for CRM-related purposes must also give customers the opportunity to withdraw consent at any time, subject to legal or contractual restrictions and reasonable notice. The company must inform the customer of the implications of withdrawing. For example, if a customer is a member of a grocery chain's loyalty program but decides that she does not want her purchase histories recorded in a database, she should have the opportunity to withdraw her consent for this use of her personal information. However, the grocery chain should also inform her that by withdrawing consent, she may not receive the cost-saving benefits provided by the loyalty program.

FIP #4: Limiting Collection

The collection of personal information shall be limited to that which is necessary for the purposes identified by the organization. Information shall be collected by fair and lawful means.

Businesses must not collect personal information indiscriminately. Both the amount and the type of information that a business collects from a customer must be limited to that which is necessary to fulfill the identified purposes of a CRM project. For example, a company that manufacturers and sells snowboards may be interested in determining the average age of its customers so it can pinpoint which media are best suited to running its ads and promotions. Consequently, it may offer individuals who buy its snowboards the opportunity to fill out a "Win a Trip to British Columbia" contest ballot that asks for a customer's name, address, phone number, e-mail address and age. For this type of CRM initiative, it would not be necessary to collect further information, such as a customer's annual income or occupation, because this information would not be necessary for achieving the purpose of the project.

Companies must only collect personal information by fair and lawful means. In other words, they should not be deceptive or misleading about why they are collecting a customer's personal information. In the above example, the snowboard manufacturer

should make it clear on the contest ballot form that it is collecting a contestant's age for marketing or media selection purposes.

FIP #5: Limiting Use, Disclosure, and Retention

Personal information shall not be used or disclosed for purposes other than those for which it was collected, except with the consent of the individual or as required by the law. Personal information shall be retained only as long as necessary for fulfilment of those purposes.

Companies that collect personal information with consent for the purpose of developing a better understanding of the needs and preferences of their customers must ensure that this information is not used or disclosed for any secondary, unrelated purposes. For example, a bank's investment arm may have a CRM project that involves collecting and updating information about the annual income and assets of its customers for the purpose of marketing investment products to them. Unless the bank obtains consent from a customer, it should not use or disclose this information for other purposes that have nothing to do with that CRM project, such as determining eligibility for mortgages or insurance products offered by the bank. Personal information that is no longer required to fulfil the identified purposes of a CRM project should be destroyed, erased or aggregated, thereby rendering the data anonymous.

FIP #6: Accuracy

Personal information shall be as accurate, complete, and up-to-date as is necessary for the purposes for which it is to be used.

The CMA's 2002 benchmark study on CRM notes that customer segments are valuable only to the extent to which they are current.[18] Consequently, personal information must be reviewed and updated on a regular basis to ensure that CRM databases reflect the present and not the past status of customers. Forty-two per cent of companies practising CRM update their customer segments on an annual basis, while another one-third do so on a quarterly or monthly basis, or even more frequently.[19]

Maintaining accurate, complete and up-to-date information about customers makes sense from both a business and privacy perspective. One aim of CRM is to enable businesses to better understand the individual needs and preferences of their key customer segments, and to serve different customers differently.[20] If a CRM database contains inaccurate or misleading information, this can have an adverse effect on a company's efforts to identify and market relevant products to its various customer groups and, conversely, may erode a customer's trust in a company.

18. Ibid., p. 43.

19. Ibid.

20. Ibid., p. 7.

Businesses may collect personal information about their customers through a variety of channels – stores, call centers, websites, e-mail campaigns, telemarketing, direct mail campaigns, or sales people in the field. A company that is implementing a CRM initiative that involves collecting or updating personal information should put policies and procedures in place to ensure that any information that is gathered is accurate, complete and up-to-date.

FIP #7: Safeguards

Personal information shall be protected by security safeguards appropriate to the sensitivity of the information.

More than 90 per cent of Canadian companies use technology to support their CRM efforts.[21] For example, sales people in the field may collect and store personal information about customers in a laptop computer or personal digital assistant and transmit this information back to the office electronically. Similarly, a customer may provide personal information electronically while filling out a website survey that a company has set up as part of a CRM initiative.

Regardless of whether personal information is stored in paper or electronic format, companies practising CRM must put in place security safeguards (e.g., locked filing cabinets for paper records), that protect such information against loss, theft or unauthorized access. The nature of the safeguards will depend on the sensitivity of the information. Highly sensitive information, such as an individual's specific income, should be accorded a higher level of protection.

CRM databases are a lucrative target for identity thieves because they contain a wealth of information about customers. To minimize this risk, access to such databases should at the very least be password-controlled and limited to those employees who need such access to perform their job duties. Companies should also take special care when destroying or disposing of personal information from CRM databases to ensure that unauthorized parties cannot access or reconstruct the information.

Privacy-enhancing technologies such as encryption can also play an important role in protecting databases from being viewed by unauthorized individuals. Encryption is a mathematical process that changes data from plaintext (which can be read) to cyphertext (an unintelligible or scrambled form). In order to reconstruct the original data or decrypt it, an individual must have access to a decryption key. Ideally, personal information should be encrypted when it is stored in a CRM database or transmitted over the Internet as part of a CRM initiative.

21. Ibid., pp. 13, 57.

FIP #8: Openness

An organization shall make readily available to individuals specific information about its policies and practices relating to the management of personal information.

The expanding scope of privacy legislation is making citizens increasingly aware and conscious of their privacy rights. According to a 2002 Harris Interactive survey, 83 per cent of American consumers would stop doing business with a company entirely if they heard or read that the company had misused customer information.[22] A Forrester Research survey of both Americans and Canadians found that almost 90 per cent of online consumers wanted the right to control how their personal information was used after it was collected.[23]

To enhance customer trust and loyalty, companies practising CRM should be open about their policies and practices with respect to the management of personal information. Customers should be able to easily acquire information about a company's privacy policies and procedures, and this information should be written in plain, simple language.

Again, best practices in privacy policies can be seen on the websites of the companies listed in FIP #3.

FIP #9: Individual Access

Upon request, an individual shall be informed of the existence, use and disclosure of his or her personal information and shall be given access to that information. An individual shall be able to challenge the accuracy and completeness of the information and have it amended as appropriate.

CRM marketers know that accuracy of information and honest dealings are mission critical components of successful customer relationships. When asked, companies must share the personal information they hold about individual customers and amend any inaccurate data. They must also provide specifics about any third parties to which they have disclosed personal information, to the best of their ability.

A business must respond to a customer's access request within a reasonable time and at minimal or no cost to the individual. It must also provide the information in a form that is generally understandable. For example, if CRM software uses certain abbreviations or acronyms to record customer information, the company must provide an explanation of what these codes mean. However, companies are not required to reveal commercially proprietary information.

22 News Release, "First Major Post-9/11 Privacy Survey Finds Consumers Demanding Companies Do More To Protect Privacy; Public Wants Company Privacy Policies To Be Independently Verified," February 20, 2002, <**www.harrisinteractive.com/news/allnewsbydate.asp?newsid=429**>.

23 News Release, "Forrester Technographics Finds Online Consumers Fearful of Privacy Violations," October 27, 1999, <**www.forrester.com/ER/Press/Release/0,1769,177,ff.html**>.

If a customer successfully demonstrates that the personal information held by the company in a CRM database is inaccurate or outdated, the company must correct the information as quickly as possible. If an individual is not satisfied that the company has properly corrected an error in his or her personal information, and the dispute cannot be resolved, the company must attach a statement of disagreement to the customer's record in the CRM database that reflects the customer's position.

FIP #10: Challenging Compliance

An individual shall be able to address a challenge concerning compliance with the above principles to the designated individual or individuals accountable for the organization's compliance.

A company must put procedures into place for accepting and responding to complaints that customers may have about its data-handling practices. The chief privacy officer or other individuals who are accountable for ensuring that the business complies with privacy legislation should take the lead in investigating and resolving any complaints. If the investigation determines that a particular CRM practice is not in compliance with the applicable privacy law, the company must take appropriate measures to remedy the situation.

Conclusion

CRM is a firmly entrenched business practice in the Canadian and American marketplace. It allows companies to provide better service to consumers and to tailor products, services and marketing offers based on the knowledge of who their customers are. Leading CRM marketers recognize the importance of building privacy and customer preferences into the system, right from the outset.

Businesses should view privacy as a tool for ensuring that CRM initiatives succeed. This can be achieved by building fair information practices into CRM, with a particular focus on being open and transparent with customers. In short, privacy is good for CRM and can help companies to gain a competitive advantage in the marketplace by building strong customer relationships based on a foundation of trust.

Privacy and Boards of Directors: What You Don't Know *Can* Hurt You

November 2003

Introduction

Today, corporate directors are faced with a wide array of responsibilities arising from their board membership. For example, directors have a fiduciary duty to act in the best interests of the corporation and a duty to maintain the standard of care. The statutory standard for the amount of care, diligence and skill required of directors is derived from the common law and codified in the *Canadian Business Corporations Act*. As a general rule, directors are required to "exercise the care, diligence and skill that a reasonably prudent person would exercise in comparable circumstances."

Increasingly, privacy is becoming one of the key issues on which directors must focus in order to execute their compliance and managerial oversight as well as mitigate risk. Privacy is often defined as the right of individuals to control the collection, use and disclosure of their own personal information (i.e., information that relates to an identifiable individual). Organizations can help to protect the individual's right to privacy by implementing what are commonly referred to as fair information practices.

New information technology, the globalization of the economy, the interconnectivity of businesses, and web-based delivery of products and services are posing new challenges to the protection of personal information. These challenges are reflected in a number of well-publicized privacy breaches. In one incident, a pharmaceutical company inadvertently disclosed the e-mail addresses of over 600 patients by sending a message to every individual registered to receive reminders about taking Prozac.

In another incident, a data management company failed to implement adequate security safeguards to prevent the theft of a hard drive containing the personal information of hundreds of thousands of Canadians. In California, a hacker was able to break into a state personnel database, gaining access to the names, Social Security numbers and payroll information of state employees ranging from office workers to judges. In Florida, personal health information was used inappropriately when free unsolicited samples of Prozac were mailed to patients using another brand of antidepressant.

Since incidents such as these can have serious consequences for both the individuals whose privacy is breached and the organization that is responsible for the breach, questions have been raised about the liability risks of directors in protecting the personal information collected, used and disclosed by their organizations.

By 2004, virtually all Canadian organizations will be required to comply with either federal or provincial privacy legislation. But, impending legislation and the potential risk of harm from privacy breaches are not the only factors compelling directors to pay closer attention to privacy issues. Research has shown that consumers are becoming increasingly concerned, better informed and more demanding with regards to the protection of their personal information. Surveys have shown that consumers will alter their purchasing behaviour if they no longer trust an organization to manage their personal information appropriately.

On some occasions, consumer backlash has forced companies to abandon plans to implement new products and services that were seen to be privacy invasive. This could happen after substantial investments have been made in the development and promotion of a product or service. Thus, it is becoming increasingly clear that the cost of mismanaging privacy can have ramifications that go far beyond legal liability.

A lack of attention to privacy can have a number of adverse consequences for which directors may be held accountable. The degree of risk will vary from one organization to the next, depending on the nature of the business and the amount of personal information that is collected, used and disclosed. The potential consequences for which a director could be liable include:

- violations of privacy laws,
- damage to the organization's reputation and brand,
- physical, psychological and economic harm to customers whose personal information is used or disclosed inappropriately,
- financial losses associated with deterioration in the quality and integrity of personal information due to customer mistrust,
- loss of market share or a drop in stock prices following a "privacy hit" resulting in negative publicity or the failure or delay in the implementation of a new product or service due to privacy concerns.

Careful attention to privacy issues may not only help directors and their organizations to avoid these risks, but may also have a number of positive effects. The potential benefits of implementing sound privacy policies and practices include:

- a more positive organizational image and a significant edge over the competition,
- business development through expansion into jurisdictions requiring clear privacy standards,
- enhanced data quality and integrity, fostering better customer service and more strategic business decision making,
- enhanced customer trust and loyalty, and
- savings in terms of time and money.

To enhance awareness of the need to protect privacy among boards, the Information and Privacy Commissioner/Ontario (the IPC) has prepared this paper for dissemination to directors. The purpose of this paper is to raise awareness of privacy not only as a compliance issue but also as a business issue. In doing so, we hope to promote the understanding that oversight of an organization's privacy compliance policies and procedures is an integral and necessary component of effective board service.

The remainder of the paper is divided into four sections. The first section describes basic fair information practices – the foundation for privacy. The second section describes the potential risks that directors and officers take when they fail to pay close enough attention to privacy in their organizations. The third section describes some of the potential benefits that can be reaped through the implementation of sound privacy policies and practices. The final section sets out recommendations for what directors should do to promote privacy compliance in their organizations. The paper concludes with a list of questions directors should ask senior management about the privacy policies and practices in their organizations to ensure privacy compliance.

What are Fair Information Practices?

Fair information practices are a set of common standards that balance an individual's right to privacy with the organization's legitimate need to collect, use and disclose personal information. In Canada, fair information practices are set out in the *Canadian Standards Association Model Code for the Protection of Personal Information* (the CSA Code). The CSA Code is incorporated into federal private sector privacy legislation, the *Personal Information Protection and Electronic Documents Act*. As of January 1, 2004, all private sector organizations in Canada that collect, use or disclose personal information during the course of commercial activity will be subject to the federal legislation, except in jurisdictions that have substantially similar provincial legislation. The province of Quebec has had private sector privacy legislation in place since 1994. The province of British Columbia has passed legislation that will come into effect January 1, 2004. The province of Alberta plans to enact legislation before the federal legislation takes effect at the provincial level in 2004.

The *CSA Code* consists of ten principles. First, it requires the designation of at least one individual who is accountable for the organization's compliance with the other nine principles (**Accountability**). The organization must specify the purposes for which it collects personal information, at or before the time when the information is collected (**Identifying Purposes**). The consent of the individual must be obtained for the collection, use or disclosure of personal information, except where it is not appropriate to obtain consent (**Consent**). The collection of personal information must be limited to that which is necessary to fulfill the specified purposes (**Limiting Collection**). Personal information must not be used or disclosed for purposes other than those for which it was collected, unless the individual consents or as required by law (**Limiting Use, Disclosure, and Retention**). Personal information must be as accurate, complete and up-to-date as necessary for the purposes for which it is to be used (**Accuracy**). The organization must implement security safeguards that are appropriate for the level of sensitivity of the personal information (**Safeguards**). The organization must make readily available specific information about its policies and practices relating to the management of personal information (**Openness**). Individuals have a right to access and request correction of their own personal information (**Individual Access**). Finally, individuals must be able to challenge an organization's compliance with the privacy principles (**Challenging Compliance**).

Directors would be proactive in satisfying their duties by assessing whether senior management has successfully implemented these practices in their organizations. A list of questions based on these principles that a director might ask is presented at the end of this document. It should be noted that the limitations placed on the collection, use and disclosure of personal information will, in many cases, require modification to existing information management practices.

What are the Potential Risks of Failing to Address Privacy?

1 Organizations that do not implement fair information practices risk violating privacy laws

As of January 1, 2004, virtually all Canadian organizations will be covered by either federal or provincial privacy legislation. The privacy rules will apply to all officers and directors of organizations covered by the legislation. Under the federal legislation, the Privacy Commissioner may initiate an investigation following a complaint or audit an organization's information management practices. The Commissioner also has the authority to publicize information about the information management practices of an organization. In addition, a complainant or the Commissioner may apply to the Federal Court for a hearing after which the court may order an organization to correct its practices; publish a notice of any action or proposed action to correct its practices; and award damages to a complainant, including damages for humiliation. The legislation puts no limit on the monetary damages that maybe awarded to a complainant.

Regardless of whether a complaint turns out to be well founded or not, it would be prudent for directors to take reasonable steps to ensure that their organizations comply with the requirements of the legislation and to avoid privacy complaints that may lead to negative publicity, damage to the organization's reputation and brand, and the payment of monetary damages to a complainant.

2 A privacy breach could be damaging to you and your organization's reputation and business relationships

A significant privacy breach could lead to unwanted publicity and additional scrutiny of you and your organization. Even in cases where media attention can be avoided, a formal complaint to the Privacy Commissioner could result in adverse information about your organization becoming public. This could lead to further unwanted scrutiny by both privacy and consumer advocates.

Directors have a duty to act with the minimum standard of care that a reasonably prudent person would exercise in similar circumstances. Directors can look to the federal privacy legislation for guidance on the standard of care that organizations should adhere to in protecting personal information. Companies and their directors may be sued for negligence if they have failed to conform to the required standard of care in their actions or inactions. Since adverse publicity arising from privacy breaches could have an impact on stock prices, shareholders may question whether the directors of an organization have conformed to the standard of care in acting or failing to act. In cases where directors were seen to fail to comply with the required standard – and it could be

argued that the actual damages from their action or inaction were foreseeable – this could lead to shareholder-initiated lawsuits.

The interconnectivity of businesses adds an additional layer of risk. Where businesses are working collaboratively on partnering and joint initiatives, privacy should be a major consideration. Businesses that have made a commitment to privacy protection will not want to expose themselves to risk through associations or partnerships with organizations that fail to conform to the required standard of care in protecting personal information.

Directors will want to ensure that privacy is a key consideration when their organizations enter into partnership arrangements, or when contractual arrangements are made with companies for the provision of specific services (e.g., information technology). An organization cannot avoid their privacy obligations by outsourcing to third parties, and maybe held liable if agents and service providers fail to comply with privacy legislation. Conversely, to avoid lawsuits initiated by business partners, directors should ensure that their organizations take reasonable steps to meet the minimum requirements for privacy protection set out in all contractual agreements with third parties and in privacy legislation.

In addition, to help minimize the damage following a privacy breach, directors should ensure that their organizations have a privacy crisis management protocol in place. The protocol should ensure that, following a privacy breach, appropriate steps are taken to minimize the damage to you and your organization's reputation and business relationships and to prevent similar breaches in the future. As part of the protocol, directors should be kept informed about all privacy breaches.

3 A privacy breach could result in serious harm to your customers

Directors need not only be concerned about the potential threat of lawsuits initiated by shareholders and business partners following a privacy incident. A privacy breach could also potentially expose you, your organization and your business partners to lawsuits initiated by customers who are the victims of a privacy breach.

Class-action lawsuits stemming from privacy breaches have emerged as a new litigation trend. In many situations, companies that have inadvertently used or disclosed the personal information of individuals without their consent have subsequently been sued. For example, in the year 2001 alone, US-based companies involved in litigation were forced to pay in excess of $60 million in settlements or judgements. In the majority of cases, judgements arose out of a failure to comply with a stated privacy policy.

Individuals may suffer a range of harms from the unauthorized or inappropriate collection, use and disclosure of their personal information. One of the more widespread harms is the unwanted intrusion into our lives from junk mail, spam and telemarketing. But, individuals can also be exposed to more serious risks including physical, psychological and economic harm. Unauthorized disclosures of seemingly innocuous personal information, such as address and telephone number, can expose some

individuals, including children, to the risk of physical harm from stalkers, abusive partners, or sexual predators.

Individuals can be humiliated or stigmatized through the disclosure of personal information relating to medical or psychiatric conditions, alcohol or drug addiction, or financial status. Unauthorized disclosures of certain types of personal information to some third parties can lead to a loss of opportunities in terms of employment, insurance, housing, and other benefits and services. Furthermore, if an organization does not take appropriate steps to guard against it, personal information that is inaccurate, incomplete or out-of-date could be used to make administrative decisions that adversely affect individuals. For example, inaccurate financial information could be used to deny an individual access to credit.

Identity theft is another growing risk that needs to be addressed. If your organization fails to implement adequate privacy and security safeguards, this may open the door to identity thieves who attempt to gain access to enough personal information to assume the identity of another person, usually for the purpose of committing crimes in that person's name. Identity thieves may go on spending sprees, take over bank accounts, open new accounts, divert financial mail, rent apartments, and apply for loans, credit cards, utilities and social benefits – all at the expense of their victims! Victims of identity thieves are often left without any credit, their reputations in ruins and may even be arrested for the crimes of the persons who impersonated them. With a poor credit rating, a victim may be denied a job, a loan, or rental housing. Average financial losses for a typical victim have been estimated to be as high as $36,000.

The Solicitor General reports that identity theft is one of the fastest growing crimes in Canada. In 2002, the PhoneBusters National Call Centre received 7,629 identity theft complaints from Canadians, with total losses in excess of $8.5 million. Canadian credit bureaus report receiving from 1,400 to 1,800 identity theft complaints each month.

Even where there is no criminal intent, it could be argued that liability for financial and other losses may be attracted, if you and your organization do not take reasonable steps to mitigate this known threat. At a minimum, these steps should include the implementation of security measures that are appropriate to the level of sensitivity of the personal information being protected. Also, in the event that there is a privacy breach, your privacy crisis management protocol should require notification of individuals whose privacy has been breached so that they may take appropriate steps to protect themselves from harmful consequences, such as identity theft.

Thus, from a risk management perspective, it is very important that directors be aware of whether their organization is being proactive in taking steps to prevent breaches from occurring – well before they arise – and to minimize the damage caused by any breaches that do occur, in spite of your organization's best efforts at prevention.

4 A lack of attention to privacy could lead to customer mistrust and deterioration in the overall quality of your organization's information assets

In today's information economy, the quality and integrity of information is critical to the success of most businesses. Accurate, complete and up-to-date information is required to provide products and services designed to meet the needs of individuals and to make informed business decisions. Organizations rely on the integrity and quality of their information. A loss of data integrity and quality will have a direct impact on your organization's ability to make sound business decisions and to provide your customers with the types of products and services that they need. Without accurate data, an organization will have no way of knowing who its customers are and how they behave. This could result in financial losses for which directors may be held accountable.

Research shows that almost all companies admit that inaccurate customer data is costing them money in terms of ineffective marketing strategies and damage to their brand and reputation. In spite of this, a large proportion of organizations do not have policies and procedures to enhance the accuracy of their customer data.

Fair information practices require that personal information be as accurate, complete and up-to-date as necessary for the purpose for which it is to be used. Adhering to this accuracy principle can have a direct impact on the quality and integrity of your information assets. In addition, implementing fair information practices can have an indirect benefit by influencing your customers' attitudes and behaviour. If customers do not feel that an organization can be trusted to handle their personal information properly, they may do a number of things: they may avoid providing complete information, withhold consent for the use and disclosure of their personal information, or worse – provide misleading or inaccurate information.

For example, research has shown that the vast majority of Internet users are concerned that the personal information they provide online will be used in an unauthorized way. As a result of this lack of trust, users rarely provide accurate personal information online. About 70 per cent of users report that they will typically abandon a website that requests personal information and about 40 per cent report having entered false information to gain access to a site.

In short, the implementation of fair information practices can help you and your organization to enhance customer trust and avoid the financial losses associated with a lack of data quality and integrity.

5 A lack of attention to privacy could result in a loss of market share and a drop in stock prices

There are a number of other ways in which a lack of attention to privacy may affect your organization's profits and stock prices. Customers who lack trust in an organization may decide to take their business to a competitor with stronger privacy practices. Mistrust and a corresponding loss of business could be the result of a failure to implement a privacy policy, the implementation of an ineffective privacy policy, specific breaches of your customers' privacy, or privacy-related incidents that attract adverse publicity.

Business could also be lost if an organization attempts to introduce a product or service without carefully considering its impact on privacy. For example, public outrage forced two companies to abandon the roll-out of a product that would have provided the personal information of 120 million American consumers on a compact disk. In the first few months following the announcement of this product, there were over 30,000 consumer inquiries and complaints. Other companies have been forced to abandon plans to embed their products with radio frequency identification devises (RFIDs) when an influential consumer group called for a consumer boycott over privacy issues inherent in what it referred to as a "smart shelf" spy system.

Delays in the roll-out of a product or service to permit privacy issues to be addressed after the fact can also be costly. For example, in one incident, a manufacturer of computer chips was forced to redesign its latest computer chip when the plan to embed a unique identification number prompted two prominent privacy groups to call for a consumer boycott of all of the manufacturer's products. Delays such as these could leave the door open for a competitor to capture greater market share. In addition, it is often far more expensive to retrofit a product or service to enhance privacy than to build in privacy protections up-front, at the design stage.

Directors who ensure that privacy is part of their organization's culture can minimize the risk of financial losses resulting from a loss of business due to customer mistrust, cancellation or delays in the roll-out of new products or services that are seen as impinging on privacy rights, and retrofitting products or services in accordance with privacy legislation and customer expectations.

What is the Business Case for Sound Privacy Practices?

1 *Sound privacy practices will give your organization a more positive image and a significant edge over the competition*

In today's highly competitive marketplace, most businesses rely heavily on brand image to differentiate their product or service from those of their competitors. Considerable resources are invested in advertising, communication, and general branding of a product or service. Negative publicity about one or more privacy breaches or poor privacy practices in general can do irreparable damage to a business's hard-earned brand image. The implementation of sound privacy policies and practices can be thought of as a kind of insurance for an organization's investment in its brand and image.

Privacy has become a business imperative emerging from the public's increased awareness of the value of their personal information. Where there are gaps in the privacy practices of competitors, privacy-sensitive consumers will choose to do business with those organizations that can demonstrate a clearer commitment to privacy and security. Thus, sound privacy practices will protect and enhance your organization's image and brand, as well as its bottom line.

2 Adherence to fair information practices can facilitate business development through expansion into other jurisdictions with privacy laws

Directors should be aware that privacy is a global issue. The original impetus for privacy legislation in Canada was the introduction of the European Union (EU) Directive on Data Protection, which prohibits the flow of personal information to countries where there are inadequate levels of privacy protection. To ensure the unimpeded free exchange of personal information across international borders, many countries have introduced privacy laws, or are in process of doing so.

In an interconnected and global business environment, weak privacy and security safeguards can impose a non-economic trade barrier to organizations that want to conduct business in jurisdictions with higher privacy standards. Awareness of international standards will help directors determine whether their organization's business practices will permit expansion into international markets.

3 Sound privacy policies and practices will allow you to customize your products and services to meet customer needs and will enhance strategic decisions

Directors should understand that customer information, lawfully collected by your organization, is a valuable asset – one that can be a useful tool in building relationships with customers. An organization's best source of information is its customers themselves. As noted previously, the integrity and quality of the personal information that your organization collects from its customers will depend on the extent to which your customers trust your information management practices. If your customers are confident that your organization will use their personal information properly, they will be more likely to share personal information that is accurate, complete and up-to-date. This will allow your organization to provide products and services that are tailored to your customers' preferences and to make sound business decisions based on the knowledge of who your customers are and how they behave.

In today's highly volatile and competitive marketplace, consumers are demanding more tailored offers for products and services, more convenience and better customer service. The Canadian Marketing Association estimated that, in the year 2000, direct marketing generated more than $51 billion in the sale of goods and services. To meet the challenges of today's business environment, organizations must know their customers intimately. Openness and transparency in information management practices and sound privacy policies provide a foundation upon which relationships with customers can be built and sustained.

4 Sound privacy policies and practices will enhance customer loyalty

As consumers are beginning to demonstrate a growing recognition of the value of their personal information and the importance of its security, the need for organizations to address privacy has become more pressing. Surveys consistently show that consumers will change their purchasing behaviour if they no longer trust an organization to manage their personal information. Whether the lack of trust stems from a publicized

privacy breach or an individual's personal experience with your organization, the damage to your bottom line may be irreparable.

Frederick Reichheld in his book, *Loyalty Rules!*, has shown that an increase in customer retention rates of 5 per cent increases profits by from 25 to 95 per cent. This is largely due to the low cost of retaining existing customers in comparison to the high cost of acquiring new customers through advertising and special promotions. Sound privacy policies and practices are one component of a good customer retention strategy.

5 A proactive approach to privacy will save you time and money

There are many ways in which a proactive approach to privacy can save you and your organization time and money. For example, you could save time and money by avoiding the following:

- lawsuits initiated by customers, shareholders and business partners,
- inquiries and complaints from your customers,
- an investigation or audit by the Privacy Commissioner,
- inefficiencies resulting from poor information management practices and the retention of inaccurate, incomplete or outdated information,
- failure of a new product or service that is seen as impinging on privacy rights,
- delays in the roll-out of a new product or service in order to address privacy concerns,and
- retrofitting of a product or service to address privacy concerns after it has been designed and implemented.

It is clear that the investment that your organization makes in preventing privacy breaches today could save you time and money spent on damage control for years to come.

What Should Directors Do?

1 Education is key – directors should ensure that they receive appropriate training in privacy and that there is some privacy expertise on their board

Directors should ensure that their knowledge about best privacy practices is current and up-to-date. Depending on the needs of the organization and those of the board, there area variety of approaches that can be taken for educating directors. For example, the board could invite privacy experts to speak at one or more of their meetings; organize a privacy workshop for directors and senior officers of their organizations, or attend one of the many privacy workshops organized by third parties.

In addition, where it is feasible, boards should establish a committee whose terms of reference include privacy. The membership of this committee should develop a degree of expertise in privacy and should be familiar with the nature and scope of the personal information collected by the organization. In order to ensure that the interests of

management do not overshadow the need for sound privacy practices, it is vital that outside directors are represented on this committee. Ideally, an outside director should chair the committee, as this will help to enhance its independence from management.

2 *Directors should ensure that at least one senior manager has been designated to be accountable for the organization's privacy compliance*

Accountability is a key fair information practice. Organizations can demonstrate accountability through the appointment of a member of senior management whose responsibilities include privacy or whose primary responsibility is privacy. In many organizations, this individual is known as the Chief Privacy Officer (CPO).

The CPO (or its equivalent) is the organization's resident privacy expert. He or she must be given the authority to oversee the design, implementation, monitoring and reporting on the organization's privacy policies and to ensure that the company's privacy compliance system and control measures comply with existing legislation. This individual should be responsible for ensuring the harmonization of privacy practices on an enterprise-wide basis. Depending upon the size and the scope of the business, the role of the CPO will vary. However, regardless of the size of the organization, the CPO has a crucial role to play – this individual must be knowledgeable about all aspects of the business.

Directors should ensure that the person appointed to carry out the functions of the CPO maintains a certain degree of separation from other senior managers of the organization. Independence will facilitate oversight of the organization's privacy policies and practices.

3 *Directors should ensure that privacy compliance is a part of senior management performance evaluation and compensation*

The designation of one or more individuals to oversee privacy compliance is not sufficient to ensure that privacy is being appropriately addressed throughout the organization. Before privacy policies and procedures can be effective, all senior managers have to make a commitment to privacy protection. Privacy compliance should be one of the criteria upon which senior managers are evaluated and compensated.

4 *Directors should ask senior managers to undertake periodic privacy self-assessments and privacy audits and to report to the board on these activities on a regular basis*

A good way to ensure ongoing privacy compliance is through regular self-assessments and privacy audits. A useful self-assessment tool is the Privacy Impact Assessment (PIA). The PIA is a systematic assessment tool designed to assess the impact of an application of new information technology or the introduction of new products and services. The PIA allows privacy issues to be identified and addressed throughout the design and implementation of a new technology, product or service. All innovations or modifications to existing information systems or products and services should undergo a PIA. Since the PIA can serve as an early warning system and risk assessment tool, directors should ensure that they receive and review all PIA reports.

Privacy audits are another useful tool that can be conducted by the CPO (or its equivalent) or by external privacy consultants. From an oversight perspective, it is preferable for the audit to be conducted by someone who is independent from the organization. The purpose of the audit is to ensure that the organization is in compliance with its own privacy policy and with existing legislation. The goal of the audit should be to promote education and awareness and to find practical solutions to everyday privacy issues. Audits should be conducted at regularly scheduled intervals, such as annually. As is the case with PIA reports, directors should ensure that they receive and review reports on all privacy audits.

5 *Directors should ensure that they ask senior management the right questions about privacy practices in their organization*

Keeping in mind the interests of shareholders and other stakeholders, including the company's employees and customers, directors have a responsibility to ensure the appropriate level of managerial oversight of privacy.

The duty of care that directors owe to their organizations entails that directors must ask the right questions of management – questions that will give management the opportunity to demonstrate compliance with both legislation and best privacy practices and generate "bottom line" advantages that result from implementing sound privacy policies. Below is a list of questions that directors may wish to ask to ensure privacy compliance.

Questions Directors Should Ask to Ensure Privacy Compliance

1 Has your organization designated at least one individual to be responsible for privacy?

2 Does your organization collect personal information? If so, would any of this information be considered to be sensitive?

3 Is the purpose for the collection of personal information explained to customers, at the time it is collected?

4 Is personal information collected only for purposes that are appropriate in the circumstances?

5 Is the personal information that is collected, used or disclosed by your organization limited to that which is necessary to achieve the specified purpose?

6 Have all necessary consents been obtained for the collection, use or disclosure of personal information?

7 Is the form of consent appropriate for the level of sensitivity of the information and consistent with the reasonable expectations of the individual?

8 Have controls been implemented to ensure that personal information is as accurate, complete and up-to-date as necessary for the purpose for which it is to be used?

9 Are the security safeguards to protect personal information appropriate for the level of sensitivity of the information?

10 Are the information management practices of the organization transparent? Does the organization make available to customers information about its policies and practices relating to the handling of personal information?

11 Do customers have the right to access and correct their own personal information?

12 Is there a mechanism through which customers can make an inquiry or complain about the organization's personal information management practices?

13 Has an organizational privacy policy been implemented? Is the privacy policy available to the public?

14 Has an employee privacy policy been implemented?

15 Has a privacy crisis management protocol been implemented to deal with privacy breaches? In the event of a privacy breach, do you communicate information to individuals whose privacy has been breached so that they may take appropriate steps to protect themselves from harmful consequences, such as identity theft?

16 Are all employees aware of the organization's privacy policy? Is privacy training, tailored to roles and responsibilities, mandatory for all employees?

17 Are privacy requirements built into contractual agreements with business partners and service suppliers and agents?

18 Are privacy requirements built into all employment contracts? Do these contracts include consequences for breaching the organization's privacy policy?

19 Does your organization conduct a privacy impact assessment prior to implementing new technologies, programs, products or services that could impact on privacy?

20 Does your organization have a compliance program that includes regular privacy self-assessments and privacy audits to ensure compliance with your privacy policy and privacy legislation?

Opening the Window to Government: How e-RD/AD Promotes Transparency, Accountability and Good Governance

June 2002

Opening the window to government

The over-arching purpose of access to information legislation ... is to facilitate democracy. It does so in two related ways. It helps to ensure first, that citizens have the information required to participate meaningfully in the democratic process, and secondly, that politicians and bureaucrats remain accountable to the citizenry.

Parliament and the public cannot hope to call the government to account without an adequate knowledge of what is going on; nor can they hope to participate in the decision-making process and contribute their talents to the formation of policy and legislation if that process is hidden from view. Access laws operate on the premise that politically relevant information should be distributed as widely as possible.[1]

Access to information is a fundamental and necessary democratic right

The values underlying freedom of information (FOI) laws, regardless of their jurisdiction, are quite simple — open, transparent, accountable and citizen-driven government. Stated simply, FOI legislation is based on a presumption that information should be widely available and accessible to the public. Governments throughout the world have recognized that citizens of a democratic state have the right to know what their government is doing, and to hold it responsible for its actions and inactions. Accordingly these rights have been enshrined in legislation providing for, and protecting, public access to government-held information.

There have been numerous reports, commissions and studies on the importance of access legislation in Canada and around the world. One seminal study was the 1980 *Public Government for Private People:* The Report of the Commission on Freedom of Information and Individual Privacy chaired by Carleton Williams for the Government of Ontario. Seven years later a federal parliamentary report was produced entitled, *Open and Shut: Enhancing the Right to Know and the Right to Privacy:* A Report of the Standing Committee on Justice and Solicitor General on the Review of the Access to Information Act and the Privacy Act. These works, and countless other government and academic papers, clearly illustrate the import and valuable roles FOI legislation play in aiding public oversight of the administration of government. Given the work that has been done in this field, it is assumed that this paper does not need to repeat these arguments, and takes for granted that the case has been made for public access to government information.

That said, statutory access rights alone are not the only reflection of an open and transparent government. A truly effective access scheme requires governments to move beyond the reactive nature of the law, and embrace routine disclosure and active dissemination (RD/AD)[2] of information as key elements of transparent and fully

1 Supreme Court of Canada - Dagg v. Min. of Finance [1997] 148 D.L.R. (4th) 385.

2 Routine Disclosure (RD) is the routine or automatic release of certain types of administrative records in response to informal requests for information rather than formal requests under FOI legislation. Active Dissemination (AD) is the periodic release of government records in the absence of a request.

accountable public administration. Furthermore, many organizations that have benefited from implementing RD/AD[3] are looking to use recent developments in information technology to advance the concept and maximize the benefits that RD/AD can offer both organizations and the public.

The Office of the Information and Privacy Commissioner/Ontario (IPC) advocates the adoption of electronic-RD/AD (e-RD/AD) in an effort to more widely disseminate government information, to provide the broadest possible public access to publicly-held information and to help reduce the barriers to access while lowering the cost and increasing the efficiency of compliance with FOI legislation.

e-Government, e-Democracy, e-Citizenship

Surveys show Canadians are active adopters and users of information technology. Canadians are world leaders in the use of the Internet, spending more time online per month than people from any other country. A study released May 23, 2001 by CF Group[4] in Toronto noted how eagerly Canadians have embraced this new medium:

- 66% of Canadian Internet users would vote online if it were possible;
- 70% of online Canadians think having government information available on the Internet makes it more available to the public; and
- 40% of online Canadians visits a government Web site monthly — with the most popular government Web sites being those related to employment, taxation and education.

These survey results closely parallel others, like the PricewaterhouseCoopers Canadian Consumer Technology Survey 2000,[5] that showed four out of every five people who go to a government Web site want information — not specific services, just information on programs and services offered by that particular ministry, agency, city or school board.

Similarly, in September 2000, a U.S. organization, the Council for Excellence in Government, released a study that found that Americans favoured government Web sites that allowed them, for example, to look up voting records, comment on federal legislation and monitor public hearings. The study, *E-Government: The Next American Revolution*[6] also asked the public to rate the most appealing aspects of e-government, and access to government services took a distant fourth. When people were asked their views on the most important of four possible benefits of e-government, access to services came last:

3 See the joint IPC/Management Board Secretariat Paper: Routine Disclosure/Active Dissemination (RD/AD) <**www.ipc.on.ca/english/pubpres/papers/rdad-e.htm**>, the related IPC Practice <**www.ipc.on.ca/english/our_role/code/practices/num-22e.htm**>, Enhancing Access to Information: RD/AD Success Stories <**www.ipc.on.ca/english/pubpres/papers/successe.htm**>, c. 06/07/01.

4 <**www.cfgroup.ca/news/01.05.23-cogm.pdf**>, c. 06/28/02.

5 <**www.pwcglobal.com/extweb/ncpressrelease.nsf/docid/6C05D8CB43319D71852569990056E0C2**>, c.06/06/01.

6 <**www.excelgov.org/egovpoll/report/poll_report.PDF**>, c. 06/06/01.

- 36% said the biggest benefit of e-gov is that government will be made more accountable to its citizens;
- 23% indicated that greater public access to information is the biggest benefit;
- 21% reported that more efficient and cost-effective government is the most desired benefit; and
- 13% felt more convenient government services are most important.

It is important to emphasize that there are a number of connected and parallel initiatives tied to the broader concept of e-government, of which e-RD/AD, while the focus of this paper, is only one aspect. It is well known that e-government has many faces including: electronic service delivery, public sector systems transformation, and digital democracy. The Canadian federal government has committed to making most of its services available online by 2004[7] while the Government of Ontario[8] wants to do the same thing by 2003 — creating a single digital window to government.[9] An example of this single window is the British government's recently announced Government Gateway,[10] a site that will eventually be the main access point to 200 central government and 500 local government institutions. FirstGov.gov is the U.S. government's portal to 30 million pages of government information, services, and online transactions.

Much of the activity around e-government[11] has concentrated on providing Internet access to government services and static general information rather than using these services to promote the goal of access to information. The purpose of this e-RD/AD paper is to stimulate thinking around moving beyond this narrow perspective and focus on bringing the widest possible range of government held information to the public.

While there are numerous groups actively promoting openness and accountability in government such as Open Government Canada[12] and the Canadian Access and Privacy Association,[13] both of which advocate for more accessible government, their efforts are often associated with politically motivated or media-driven interests. The United States has a virtually limitless number of organizations and associations that fight on behalf of FOI access. Space does not permit for a broad philosophical discussion of the differing approaches to FOI in Canada and America. However, a brief

7 <**www.gol-ged.gc.ca/index_e.asp**>, c. 06/06/01.

8 <**www.cbs.gov.on.ca/mcbs/english/56HK6V.htm**>, c. 06/28/02.

9 The government has noted that e-gov provides "Stronger Accountability" and "improved access to information."

10 <**www.gateway.gov.uk**>, c. 06/06/01.

11 There are a number of initiatives promoting e-democracy and e-citizenship. One significant Canadian initiative is the Crossing Boundaries project led by Winnipeg South M.P. Reg Alcock <**www.crossingboundaries2.com**>, c. 06/06/01. However, projects intended to "reconnect" citizens and elected officials using technology do not typically address FOI primarily, but rather focus on providing electronic services or creating a new sense of "digital democracy" and attempting to cross the "digital divide" between technological have and have nots.

12 <**www.opengovernmentcanada.org**>, c. 06/06/01.

13 <**www.capa.ca**>, c. 06/06/01.

analysis of the FOI laws in practice in the United States is instructive for how that country's perspective on public access to government information could provide some direction to our own initiatives. This paper also will highlight some recent Canadian FOI-related initiatives at the federal level, as they could have a positive effect on the way FOI matters are viewed and handled in Ontario.

Examples of e-FOI in action

In 1993, then U.S. President Clinton sent a memorandum to all heads of federal departments and agencies, calling upon them to "renew their commitment to the Freedom of Information Act, to its underlying principles of government openness, and to its sound administration." The President noted that the FOI legislation was "based upon the fundamental principle that an informed citizenry is essential to the democratic process and that the more the American people know about their government the better they will be governed." Most importantly, the President concluded that:

> [O]ur commitment to openness requires more than merely responding to requests from the public. Each agency has a responsibility to distribute information on its own initiative, and to enhance public access through the use of electronic information systems. Taking these steps will ensure compliance with both the letter and the spirit of the Act.[14]

A memorandum, similar in tone, by Attorney General Janet Reno, accompanied the President's. The spirit of FOI remained strong in Washington following these executive memoranda and was reflected in the 1995 *Paperwork Reduction Act* and the 1996 *Electronic Freedom of Information Act Amendments* (E-FOIA).[15]

The E-FOIA legislation requires agencies post on their Web sites and make available through electronic reading rooms, all records that have been requested under the Freedom of Information Act in the past, and that have been, or are likely to be, subject to additional FOIA requests. This has resulted in the most popular and frequently requested records being available to the public without the need to submit a formal FOI request. The E-FOIA also required agencies to index all of their records and make these indices available online (similar to Ontario's Directory of Records).[16] These indices enable the public to describe, with greater accuracy, the records sought and decrease agency response time by making it easier to search for and identify the requested records.

14 <**www.citizen.org/litigation/foic/clinton_94.html**>, c 06/06/01.

15 While the Reno memo has been "superseded" by October 12, 2001 memo from Attorney General John Ashcroft emphasizing the importance of safeguarding government information and changing standard of review from "foreseeable harm" to a lower standard of "sound legal basis," one can only hoped that this response will be limited to these particular tense times after the events of September 11, 2001. However, given the development of a new category of information assigned by the Information Security Oversight Office of "Sensitive But Unclassified Information" and the on-going efforts to remove significant amounts of information that was previously publicly accessible, the evidence would suggest that FOI has been seriously impacted, at least in the short term, by concerns over national security and public safety. See also *Access and Privacy: A Balancing Act:* a speech given by the IPC's Greg Keeling to Open or Controlled Society? Access to Public and Corporate Information: A Civic Conference <**www.ipc.on.ca./english/pubpres/speeches/051002gk.htm**>.

16 <**www.cfipo.gov.on.ca/mbs/dor/dirrec.nsf/webpages/main**>, c. 06/06/01.

Enacted the year before E-FOIA, the *Paperwork Reduction Act* gave specific responsibilities to the Office of Management and Budget's (OMA) Office of Information and Regulatory Affairs (OIRA) to ensure that:

- effective and efficient information resource management practices are implemented across the government;
- the paperwork burden imposed by the federal government on the public is minimized; and
- the greatest possible public benefit comes from the collection, use, and dissemination of information collected from the public.

The OMB subsequently reported to Congress on the operation of the statute. In the September 1997 report, the OMB included a chapter on Government Information and Services: Information Dissemination Activities and Trends.[17] The report noted the Clinton Administration's goal of using information technology to "make it easier for users of information, including citizens, scientists, resource managers, and private industry" to find the specific government information they need. The chapter concluded by stating:

> [R]ecent advances in web and related search technology to make increasing amounts of electronic information more manageable ... reflects an unprecedented level of attention to the development of information dissemination practices that both integrate the vast information holdings of the Government and at the same time make them more accessible and useful to the public.

The importance of executive level support for initiatives such as the Paperwork Reduction Act and the E-FOIA legislation cannot be overstated. Bolstered by these legislative initiatives and program reviews undertaken by organizations such as the Government Printing Office,[18] the discussion of public access to information has remained high on the political agenda over the years. We have recently seen a renewed interest in public access to information. In January 2001, the U.S. National Commission on Libraries and Information Science (NCLIS) released *A Comprehensive Assessment of Public Information Dissemination*.[19] In this report, NCLIS recommended, "the United States Government formally recognize and affirm the concept that public information is a strategic national resource." The report called for the creation of an independent Public Information Resources Administration to be the lead agency for information policy and dissemination; similarly, there should be separate Congressional and Judicial Information Resources Offices.

The NCLIS report noted that, "Public ownership of information created by the federal government is an essential right. It not only allows individuals to fulfil their civic

17 <**www.whitehouse.gov/omb/inforeg/prarep3.html**>, c. 06/28/02.

18 Report on the Assessment of Electronic Government Information Products <**www.access.gpo.gov/su_docs/nclisassessment/report.html**>, c. 06/06/01.

19 <**www.nclis.gov/govt/assess/assess.html**>, c. 06/06/01.

responsibilities, but also contributes to an overall improvement in their quality of life." The report highlighted a range of difficulties people have with online information including the accessibility of the resources required to get electronic files, the seeming ephemeral nature of electronic documents and a lack of a long-term access and storage solutions for such material.

A few months after the NCLIS report, the United States General Accounting Office released a Report to Congressional Requesters entitled, *Information Management - Progress in Implementing the 1996 Electronic Freedom of Information Act Amendments*.[20] The report found that while many of the provisions of the E-FOIA legislation had been enacted, there was still much work to be done.

Countering some of the indications of a pullback on FOI noted earlier however, the U.S. government nonetheless appears to be pushing ahead with e-government initiatives, recently passing the E-Government Act of 2001. This legislation establishes an online director of federal Web sites, requires federal courts to post opinions online, and requires agencies to post rule-makings online.

Closer to home, the Canadian Federal Access to Information Review Task Force[21] is reviewing the functioning of the access legislation. Task Force Chair Andre Delagrave recently stated that the consultations are looking into a number of issues, including:

- integrating access with other measures of transparency and accountability;
- technology applications to facilitate the access process;
- routine proactive disclosure;
- new approaches to policy making that are compatible with early disclosure;
- modernizing records management; and
- creating a culture of access.

While this Task Force indicates that it is reviewing the types of issues that are consistent with an e-RD/AD approach, only time will tell if its efforts were worthwhile.[22] However, should the review promote the important values of e-RD/AD, then it can be viewed as at least a partial success. It is hoped that these types of reviews also will look at the accessibility of non-digital records as, currently, the vast majority of historical government files are stored in non-electronic formats such as paper, microfilm, microfiche. Similarly, a great deal of data resides in difficult to access storage media such as older format data tapes, disconnected data drives and the like. Archivists have been discussing the issue of long-term storage and indexing of electronic media for years

20 <**www.gao.gov/cgi-bin/fetchrpt?rptno=GAO-01-378**>, c. 06/06/01.

21 **<www.atirtf-geai.gc.ca/home-e.html**>, c. 06/06/01 A number of comprehensive and stimulating submissions have been made to the Task Force and provide useful insight into some of the ways that broader access to government information could benefit society.

22 See the IPC's submission <**www.ipc.on.ca/english/pubpres/reports/info0501.htm**>, c. 06/06/01.

without coming to any clear consensus on how to proceed.[23] We also would be remiss if we did not point out the important public access role played by public archives[24] and the federal and provincial depository library programs.[25]

e-Government and e-RD/AD in Ontario

In the April 19, 2001 Speech from the Throne, the Government of Ontario noted that public sector organizations must be accountable to the public. The Speech stated: "Government is the servant of the people, not master. Citizens are more than "customers" or "clients;" the entire public sector belongs to them. Citizens are entitled to transparency in the operation of public institutions..."[26] As part of the this focus on customer service and e-government, an announcement was released noting in part:

> The government will become a world leader in electronic service delivery by giving citizens seamless and convenient access to government information services. Individuals and businesses will have greater choice about how, when and where they access routine government information, perform transactions, obtain advice and purchase products. They will be able to evaluate the quality of service themselves [emphasis added].[27]

This announcement of an intention to provide better public access to information is encouraging and supports the goals of e-RD/AD. We suggest that any fully scoped e-government initiative should address two broad areas: providing better services to the public, and re-establishing the relationship between citizens and those whom they elect. The development of e-RD/AD as an integral component of electronic government services, can build on the best practices of existing RD/AD initiatives in Ontario while learning from American and European experiences.

A number of examples of successful e-RD/AD efforts already exist. The Region of York's water quality reports can be now be found on its Web site. The City of Toronto publishes health inspection results of restaurants on the city's Web site. The cities of Waterloo and Mississauga routinely make a variety of information available including Council and Committee agendas, meeting minutes and municipal bylaws. The City of Brampton has incorporated a proactive RD/AD policy that has become a standard feature of the City's operating procedures. This policy includes: FOI trend analysis to determine which requests could become RD/AD material; a corporate file classification manual in which records are tagged for RD/AD retention; and active Web publishing. Provincially, the

23 See NCLIS's "Assessment of Formats and Standards for the Creation, Dissemination, and Permanent Accessibility of Electronic Government Information Products" <**www.nclis.gov/govt/gpo1.html**>, c. 06/07/01.

24 Ontario's former Provincial Archivist Ian Wilson said, "If you really want to run a government that isn't accountable, you don't keep any records. But if a government is to be accountable to the people, then we need good records of the key events, decisions and policies." <**www.ipc.on.ca/english/pubpres/newslet/spr95.htm**>, c. 06/06/01.

25 See <**www.nlc-bnc.ca/6/1/s1-300-e.html**>, c. 06/06/01.

26 <**www.premier.gov.on.ca/english/library/thronespeech-Apr1901.htm**>, c. 06/06/01.

27 <**www.cbs.gov.on.ca/mcbs/english/4W3MUL.htm**>, c. 06/07/01.

Ministry of Environment began posting a wide range of water-related information, including boil water advisories, after the tragedy in Walkerton.[28]

These efforts only hint at the potential opportunities for e-RD/AD at the municipal and provincial levels. The principles behind FOI and RD/AD are not just about democratic rights or good government practice; they are at the heart of an individual's connection with their government and elected officials. The old adage that "information is power" has never been truer. In order to keep power in the hands of the people, e-RD/AD initiatives are not only good practice, they are critical to the ongoing health of our democratic system – especially when an increasing number of people appear to be disconnected from the institutions of government.

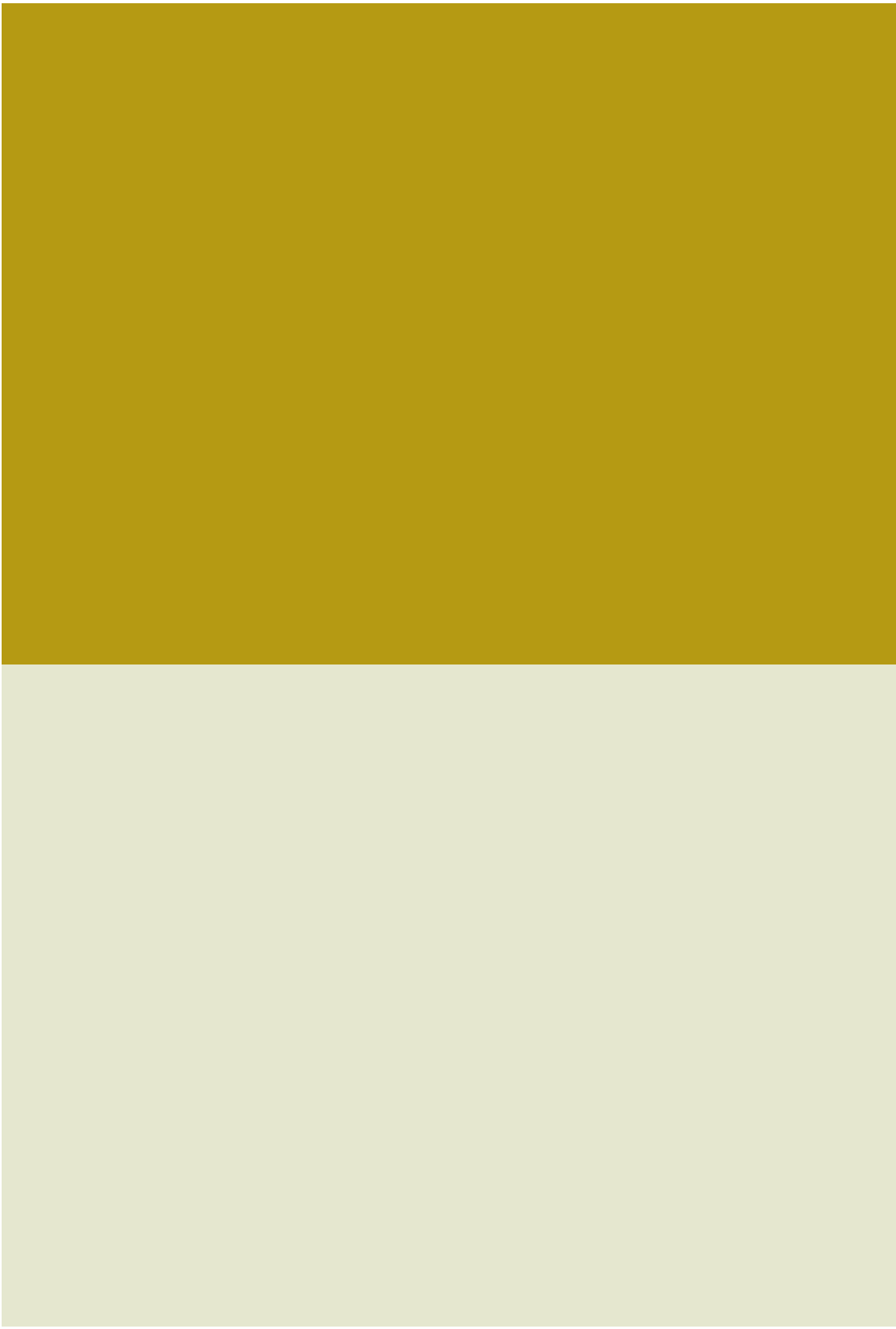
The IPC is committed to advancing the concept of e-RD/AD and has featured the topic in our 2000 Annual Report.[29] Through concerted efforts, the limited FOI resources of public institutions can be leveraged by using e-RD/AD and will result in lower administrative costs, higher service quality, and an improved relationship with the public and interested stakeholders.

28 <**www.ene.gov.on.ca/water.htm**>.

29 <**www.ipc.on.ca/english/pubpres/ann_reps/ar-00/ar-00e.htm**>, c. 06/12/01.

Privacy Diagnostic Tool (PDT)

August 2001



Introduction

In January 2000, the *Wall Street Journal* published a survey that showed privacy as the number one concern for North Americans for the 21st century. More recently, on March 5, 2001, Forrester Research completed a study of privacy issues for business. They stated that, "Anyone today who thinks the privacy issue has peaked is greatly mistaken … we are in the early stages of a sweeping change in attitudes that will fuel political battles and put once-routine business practices under the microscope."

At the same time, advances in information technology and the Internet have changed the way that companies do business. Over the past decade, we have seen unparalleled growth in the ability of organizations to collect, compile, analyze, and disseminate personal information, not to mention the unprecedented volume of personal information that organizations routinely collect. As the *Wall Street Journal* and others attest, consumers expect their personal information to be protected and their privacy to be respected by the organizations they do business with. Breaching consumer expectations or breaking their trust lands organizations on the wrong side of the privacy issue.

Today, leading businesses recognize that privacy concerns threaten the bottom line. Accordingly, addressing privacy concerns effectively is beginning to be seen as a winning strategy for both business and consumers.

What is Privacy and Why Does It Matter?

A wide variety of interrelated values, rights, and interests come together under the rubric of privacy. For most businesses, however, the most relevant sub-set of privacy is informational privacy (also known as data protection).

Information privacy is the ability of an individual to exercise a substantial degree of control over the collection, use, and disclosure of their personal information.

Personal information includes any information about an identifiable individual. This includes information such as name, address, gender, age, ID numbers, income, ethnic origin, employee files, credit records or medical records. An individual's name need not be attached to the information in order for it to qualify as personal information.

Most companies need to collect, use and disclose some information about their customers in order to conduct their business. But organizations must be reasonable and fair in their treatment of personal information, not only for the good of their customers, but also for the good of their own business reputations. Consumers are no longer willing to overlook a company's failure to protect their privacy. High profile misuses of personal information have shown that a lack of respect for personal information can bring both harsh criticisms from consumers, and significant devaluation of company shares.

Thanks in part to much publicized incidents, many jurisdictions have seen a wave of legislative initiatives, such as the European Union Directive on Data Protection and Canada's *Personal Information Protection and Electronic Documents Act* (PIPEDA).

Organizations around the world are now beginning to take note of international and local regulatory initiatives that may influence how they treat customer information.

There is no better time than the present for organizations that handle personal information to take a close look at their practices and bring them into line with emerging consumer expectations. In the short term, protecting personal information and developing consumer trust promise to become a strong competitive advantage. In the long term, protecting privacy will become a new business imperative.

The Privacy Diagnostic Tool (PDT): What's In It For Me?

Organizations interested in doing business must take data privacy issues very seriously. According to a Senior Executive Panel at the May 2001, *Computerworld* Premier 100 Conference, even one privacy slip-up could be devastating to a company's corporate image and brand.

Can an organization benefit from paying attention to the PDT and taking the time to use it? To help you and your organization decide whether or not to use the PDT, please review the following questions. If your organization answers yes to one or more of these questions, you will benefit from using the PDT. In fact, we highly recommend it.

Questions

1. Does your organization collect and use personal information in the course of your business?
2. Is the use of personal information an important part of your business (for example, as part of marketing, sales or Customer Relationship Management)?
3. Do you disclose your customer's information to anyone?
4. Have you bought, sold, traded or shared personal information?
5. Is your organization potentially vulnerable to internal or external security breaches involving your customers' personal information?
6. Do you have any questions on how current or upcoming privacy regulations will affect the way you collect and use personal information?

If you answered yes to one or more of the above questions, you will benefit from using this Privacy Diagnostic Tool.

NOTE: For a comprehensive list of all the questions in the Privacy Diagnostic Tool please visit our website at **www.ipc.on.ca**.

Using the Privacy Diagnostic Tool

The PDT is a voluntary, self-administered assessment of whether and to what extent your business's information management practices are privacy-friendly. Working through a series of questions, the PDT will help you to both assess and educate your organization, ensuring a better understanding of how to protect personal information and build consumer trust.

The PDT addresses ten principles that are key to the proper management of personal information, based on internationally recognized norms known as Fair Information Practices (FIPs). FIPs are overlapping and cumulative principles that outline responsible information handling practices. They cover the following areas:

- Accountability
- Identifying Purposes
- Consent
- Limiting Collection
- Limiting Use, Disclosure, Retention
- Accuracy
- Safeguards
- Openness
- Individual Access
- Challenging Compliance

The PDT outlines each principle, explains its objectives, and notes some risks that your organization may face if it fails to adhere to the principle.

For each principle, there is a series of questions on implementation, divided into two sections. The first section, *Implementing the Principles*, identifies and assesses your compliance with the *required* steps for implementing the principle. The second section, *Best Practices*, identifies and assesses your compliance with best practices for implementing the principle. Simply answer *Yes* or *No* to each question, based upon your current business practices. If the requirement or best practice is not applicable to your organization, answer *Yes*.

If you have answered *No* to one of the questions under the heading *What You Need to Do*, your organization is not fully adhering to that Fair Information Practice. You should review and amend your policies and procedures to ensure a *Yes* response. If you answered *No* to any of the best practices, consider whether you should adopt this practice in your organization.

About the Privacy Diagnostic Tool

Please note that this tool is not designed to provide a detailed privacy audit or an in-depth privacy impact analysis. Use of this tool should be viewed as an initial gauge of one's privacy readiness – it is intended to be complimentary to other measures you might take to protect privacy and to any measures you may be required to take for compliance with privacy legislation and other legal standards or industry privacy codes applicable to your organization.

We have endeavoured to make this tool as useful as possible. However, the Information and Privacy Commissioner/Ontario (IPC) takes no legal responsibility for the results of using this tool. The information contained in this publication should not be considered legal, accounting, tax or other professional advice or services. (If you need specific advice about your particular situation, you should always consult a suitably qualified professional).

The PDT has been developed by the IPC with the generous assistance of Guardent and PricewaterhouseCoopers. Any errors or omissions are the sole responsibility of the IPC.

The PDT is available free of charge to any company that wishes to examine its information management policies, or to consumers who may want a tool to analyze the privacy practices of the businesses with which they interact. It is also designed to be completed anonymously and does not require the provision of results or information to any of the developers.

Privacy and Biometrics: Friend or Foe?

September 1999

Abstract

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

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

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

Introduction

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

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

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

Privacy Friend or Foe?

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

When considering the privacy concerns associated with biometrics, an important distinction must be made between identification and authentication. A computer system can be designed to identify a person based on a biometric characteristic. To do this, it compares a biometric presented by a person against all biometric samples stored in its

database. If the presented biometric matches a sample on file, the system has identified the individual. This is called a "one-to-many" match, and is used by the police to identify criminals, as well as by governments to identify qualified recipients for benefit-entitlement programs and registration systems such as voting, driver's licenses and other applications.

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

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

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

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

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

The threat to privacy arises not from the positive identification that biometrics provide best, but the ability of third parties to access this data in identifiable form and link it to other information, resulting in secondary uses of the information, without the consent

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

of the data subject. This erodes the personal control of an individual over the uses of his or her information. Informational privacy is defined as the ability to maintain control over the use and dissemination of one's personal information. It revolves around freedom of choice and personal control — informational self-determination.

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

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

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

Biometrics and Government Programs

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

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

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

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

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

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

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

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

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

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

Further, the statute includes the following provision:

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

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

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

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

Biometrics and Policing

The IPC contributed a chapter on biometrics and policing to the proceedings for the Sommerakademie 1999 in Kiel, Germany.[4] In that document, the IPC recognized the potential harm from the misuse of biometrics as significant, but further argued its

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

position that the key point for discussion about biometrics was not that the technology should not be used because it posed a threat to privacy, but rather, when used, it must be used responsibly.

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

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

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

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

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

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

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

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

Biometrics and Consumer Applications

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Conclusion

Two things are certain:

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

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

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

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

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

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

407 Express Toll Route:
How You Can Travel the 407 Anonymously

May 1998

Objective

The Ontario Transportation Capital Corporation (OTCC) and the Information and Privacy Commissioner/Ontario (IPC) wish to raise the public's awareness as to how one can travel along the 407 Express Toll Route (407 ETR) — an electronic toll highway, and still maintain their personal privacy.

Introduction

When the IPC first learned that the 407 ETR was going to use electronic technology to collect data on highway users for purposes of automatic billing, the OTCC was contacted to discuss the privacy issues involved. At the initial meeting in May 1994, the OTCC assured the IPC that the need to protect personal privacy was already included as part of the Highway 407 Project Request For Proposals (September 1, 1993). The OTCC had recognized the importance of including privacy in all aspects of the design and operation of the highway. In addition to ensuring that any personal information collected on highway users would be used for billing purposes only, the OTCC developed a unique billing system that allows individuals the opportunity to travel the 407 ETR and pay for their trips without having to reveal who they are.

A significant amount of work was required to ensure that the 407 ETR toll and billing system did not compromise personal privacy. In order to accomplish this goal, a number of toll billing programs and routines were developed. Most important, however, were the special arrangements made for alternative payment methods with financial institutions to collect toll payments without the requirement for any personal identifiers — an anonymous account, a most unusual occurrence. The 407 ETR staff then needed to be trained to deal with members of the public enquiring about opening an anonymous account.

A considerable amount of effort was expended by the OTCC staff and its private sector partners to ensure that 407 ETR anonymous accounts would be available to the public. The effort was well worth it — the public now has a means of travelling the 407 ETR in a manner that protects the privacy of highway drivers.

What is the 407 ETR?

The 407 ETR is a multi-lane toll highway, running 69 kilometres across the top of the Greater Toronto Area. What places it apart from other toll highways is its use of high-tech toll technology. It is the world's first completely electronic toll highway — a state-of-the-art transportation route that will move people and goods efficiently without any toll booths or plazas. Tolls are calculated based on time of day, day of the week, distance travelled, and class/weight of vehicle, all collected using electronic technology.

When you enter one of the 29 interchanges on this highway, you simply drive under an overhead tolling gantry that automatically records the beginning of your trip into the 407 ETR's electronic toll collection system. When you exit the highway, you drive under another overhead frame and the toll system logs your vehicle off the highway.

How does it do this? The 407 ETR uses a suite of technologies commonly referred to as "Intelligent Transportation Systems."

Intelligent Transportation Systems

For an in-depth discussion of this suite of technologies and their privacy implications, we refer you to the IPC's paper entitled, *Intelligent Transportation Systems and Your Privacy*, published in 1995. A brief overview of Intelligent Transportation Systems technology is provided below.

Intelligent Transportation Systems (ITS) is the name for a group of technologies specifically designed to reduce traffic congestion and to improve highway efficiency, safety, and convenience. ITS may involve any of the following:

- All types of vehicles, including private cars, taxis, trucks, buses, and trains;
- All aspects of surface transportation systems, including urban and rural roads, freeways, transit stations, and ports;
- A variety of information devices, such as computers, signs, dashboard monitors, hand-held equipment, and kiosks.

Although some ITS applications are still in the developmental and testing stages, there are many which have already been implemented. These include electronic toll roads and changeable message signs (electronic message boards located over the highway that alert drivers to road or weather conditions ahead).

Toll Roads in Other Jurisdictions

Several large scale projects have either been developed or are under way in the United States, United Kingdom, Portugal, Italy, Finland, Sweden, Norway and Singapore. One of the more interesting examples is presented below.

In the United States, the SR91 Express Lanes in California is said to be the world's first fully automated highway using transponders to collect tolls electronically. While this road is ten miles long, it essentially has only one entry and one exit point, very much like a long bridge. Today more than 30,000 transponders are in use on this highway and it has alleviated congestion on its adjacent freeway.

To date, none of the toll roads in other jurisdictions that use transponders to collect tolls electronically offer motorists the option to travel the road anonymously. In all cases, patrons of these toll roads must identify themselves to the toll system in order to obtain a transponder. Ontario's 407 ETR represents a first globally — to date, it is the only highway of its kind that provides its customers with a way to travel their toll road without compromising their privacy.

Ontario's 407 ETR and ITS

The 407 ETR's toll collection technology has five main components: the vehicle recognition and identification system, the vehicle transponder, the roadside toll collection system, the toll transaction processor, and the revenue management system.

For users of the 407 ETR who do not have a transponder, tolls will be collected and calculated using a rear licence plate recognition and identification system. A transponder is a device roughly the size of a garage door opener that is attached to the inside of the vehicle's front windshield (behind the rear view mirror). When a vehicle without a transponder enters and exits the highway, a video camera records the vehicle's rear licence plate and sends the image to a central processing computer to be matched. The system checks its database to determine if an account exists for this licence plate number. If not, an electronic search is made of the province's vehicle licence database for the name and address of the registered licence plate holder to allow an account to be set up. The toll is calculated using a billing rate table and an invoice is sent to the registered licence plate holder in the mail once a month.

Regular highway users are encouraged to register and obtain a transponder. For vehicles with a transponder, the plate recognition and identification system is not activated. When a vehicle equipped with a transponder enters the highway, the transponder logs that vehicle onto the 407 ETR's electronic toll collection system at the start of the trip. Upon leaving the highway, the transponder is read by another overhead electronic sensor to complete the toll transaction. Using the same billing rate table, a toll is calculated and a bill sent out on a monthly basis. Unique among toll authorities, OTCC introduced a number of payment options including pre-payment, post-payment, pre-authorized bank withdrawal, or charging to one's credit card.

Why Ontario's 407 ETR is Different from Other Jurisdictions

There are three privacy components that set Ontario's 407 ETR apart from other toll roads. First, the plate recognition system only records the rear licence plate of the vehicle. Thus, no images of the vehicle's occupants are recorded or collected. The OTCC agreed with the IPC that it was not necessary to obtain pictures of the front plates of passenger cars for toll-collection purposes.

Second, legislation only permits the OTCC to use any personal information it collects for two purposes: toll collection and traffic management. The OTCC does not allow any secondary uses of this personal information without the consent of those involved (e.g., for promotional material).

Third, and most important, is the option of obtaining a transponder and travelling the highway anonymously, without providing any personal information — ever. To open a *regular transponder account* individuals must provide some identification during the registration process in order to effect the following monthly payment options: they can be billed by mail, they can have a preauthorized bank withdrawal, or they can have a pre-authorized credit card charge. In all of these instances, individuals must supply a certain amount of personal information to have these arrangements made.

However, with an *anonymous transponder account*, an individual is not required to provide any identification whatsoever. All financial transactions are done via cash to ensure true anonymity. During the registration process, no personal information is required —

an account is opened and a security deposit is prepaid by cash.[1] When the IPC first presented the anonymous option, the OTCC's initial proposal required anonymous account clients to visit the OTCC Operations Centre to replenish their account, whereas regular transponder account clients could pay through a variety of means. Since it was important that the anonymous transponder option be as convenient to use as the regular transponder option, this solution was not acceptable to the IPC. The OTCC then explored the idea of having anonymous transponder clients replenish their account at any chartered bank or trust company, without providing any identification. Through extensive discussions with the financial community, the OTCC was successful in achieving this objective.

The method of payment developed for anonymous accounts is unique: the user's OTCC account (not a bank account but just like one, for an account holder's purposes) is credited with funds for future trips on the 407 ETR — in effect, a prepaid cash account. This is accomplished by using a preprinted payment booklet. When an anonymous account is first opened and a transponder issued, the individual is also provided with a booklet of payment slips that are preprinted with the anonymous account number. When it comes time to replenish their account (learned through the transponder which signals the driver by a flashing yellow light and one beep), one simply visits any chartered bank or trust company and deposits funds into the account number that appears on the payment slip. The clerk at the financial institution marks the payment slip with the amount of money paid and then electronically transfers the funds to the OTCC account. The bank or trust company acts as a convenient intermediary, accepting deposits into anonymous accounts on behalf of the OTCC. Payment can also be made by mail or in person at the 407 ETR Operations Centre where a similar electronic transfer of funds will occur.

If they wish to remain anonymous, anonymous transponder users cannot let their account balances fall to zero (transponder signals this by a red light and one beep). If they do, a record of the trip and any others will be made using the rear licence plate recognition and identification system and a bill will be mailed to the registered licence plate holder. Thus, anonymity is forfeited if accounts are not replenished. However, patrons are given sufficient warning so as to allow enough time to replenish their anonymous accounts.

Vehicles Over 5 Tonnes

Anonymous accounts are available for 'light' vehicles only, which include cars, vans, and pickup trucks. For vehicles with a Registered Gross Vehicle Weight or Gross Vehicle Weight over 5 tonnes, transponders are mandatory under the *Highway Traffic Act* (Ontario) in order to travel the 407 ETR. These 'heavy' vehicles, which include large trucks, dump trucks, tractor trailers, etc., require a transponder for a number of reasons including:

1 A form of security deposit is required from everyone obtaining a transponder.

1. The rear licence plate of any trailing vehicle is not necessarily registered to the driver/owner of the power unit (permit holder of tractor). Therefore, reading the trailers' licence plate would not provide the information necessary to forward the toll charge invoice to the registered plate holder;

2. The toll system is presently designed to take video images of rear licence (trailer) plates. For heavy vehicles, these plates may be recessed or be in unusual locations which the system cannot reliably read;

3. The OTCC recognizes the need to ensure an even playing field for all commercial vehicles. The province wants to ensure that Ontario's commercial trucking industry is not put at a competitive disadvantage vis-a-vis out-of-province commercial vehicles who may attempt to evade paying tolls. Thus, the requirement for mandatory transponders for all vehicles with a Registered Gross Vehicle Weight or Gross Vehicle Weight over 5 tonnes.

To ensure that tolls are collected from all heavy vehicles, the OTCC uses two toll collection methods available through the current 407 ETR tolling system. The primary means to identify a heavy vehicle which does not have a valid transponder is through the rear licence plate recognition and identification system. A supplementary toll collection method for non-transponder heavy vehicles accurately identifies toll violators through the front licence plate. This secondary toll collection process is not unduly invasive since no passenger vehicles are recorded.

This secondary system will be made up of permanent sites as well as portable units which will be continually relocated along the 407 ETR to gain maximum toll collection potential. Heavy vehicles found to be on the highway without a valid transponder will be sent a toll charge for the trip taken and an additional $25 Heavy Vehicle Non-Transponder Toll Charge. As well, if the Ontario Provincial Police or Ministry of Transportation Enforcement Officers stop a heavy vehicle on 407 ETR without a valid transponder, the driver will be subject to a $90 *Highway Traffic Act* fine.

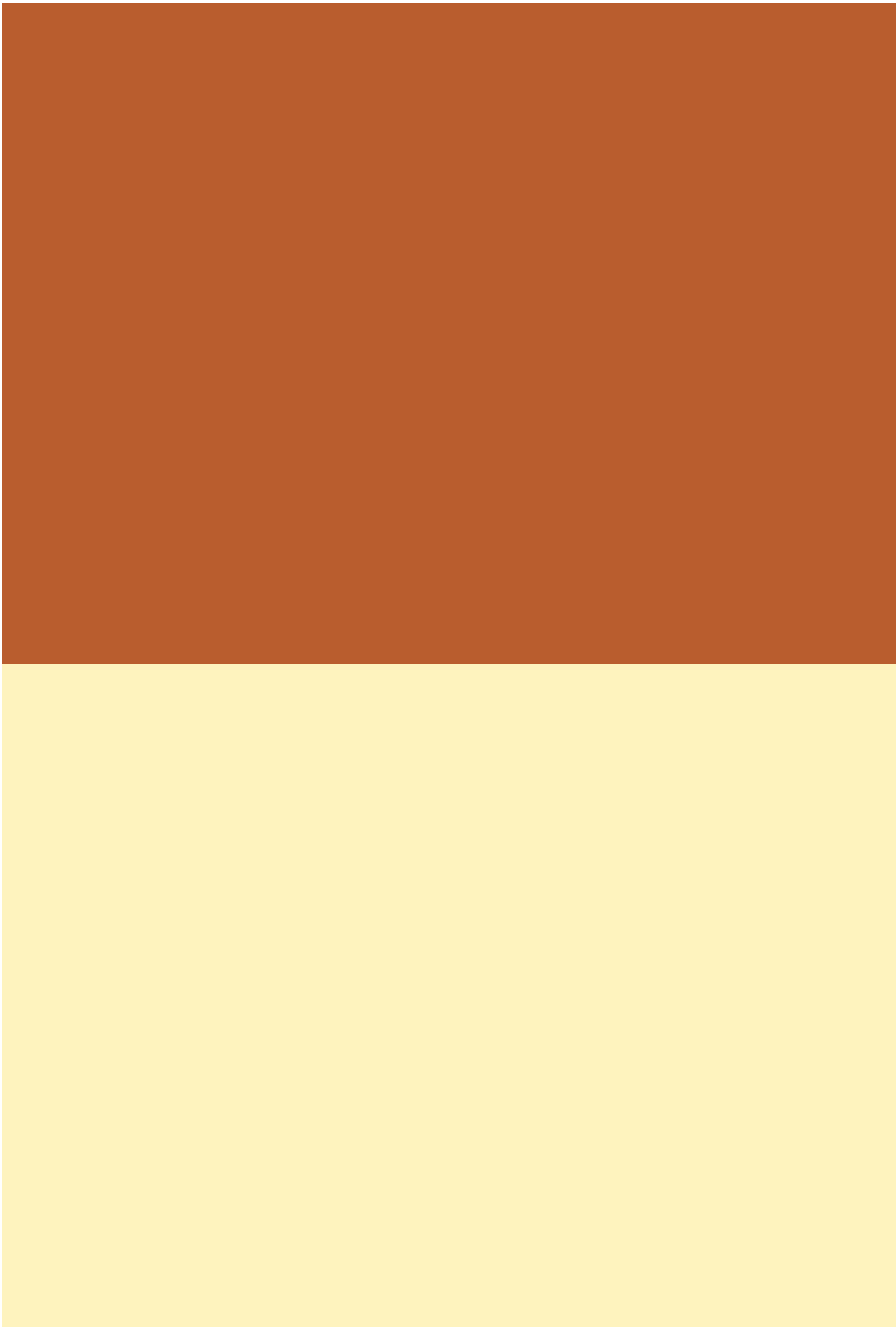
Conclusion

While Intelligent Transportation Systems have the capability of being privacy invasive, when coupled with the will to preserve privacy, they can become privacy enhancing. The OTCC and the IPC have worked together from the outset of this initiative to ensure that privacy was considered throughout all phases of the development and implementation of this project. Through this cooperation, we have ensured that the public has a way in which to travel the 407 ETR in an anonymous manner. We consider this a true win/win scenario.

Please visit our website, **www.ipc.on.ca**, to view all the detailed questions (and answers) in this publication that individuals may have regarding the use of personal anonymous transponders.

Data Mining: Staking a Claim on Your Privacy

January 1998



Preface

Globally, issues about informational privacy in the marketplace have emerged in tandem with the dramatic and escalating increase in information stored in electronic formats. Improvements and innovations in computer processing power, disk storage, and networks have been close to explosive. Very large databases with transactional information about every aspect of business are now measured in gigabytes and terabytes. Fuelled daily by massive amounts of data, the data volume is so huge that it has been estimated that businesses can only use seven per cent[1] of the data collected.

Much of this large mass of data is donated by the consumer in the course of conducting his or her daily personal business: withdrawing cash from ATMs; paying with debit or credit cards; using loyalty cards; borrowing money; writing cheques; renting a car or a video; making a telephone call or an insurance claim; and, increasingly, sending or receiving e-mail and surfing the Net. Since virtually all of these transactions or activities involve some form of electronic identification, each transaction captures some personal information about you and stores it in electronic form.

Speed, convenience, easy access, discounts, bonuses, awards, frequent flyer points — all of these have encouraged or eased the transition from social interaction to electronic interaction. Often, there is no longer a choice to be made, or if there is a choice, it will rarely match the speed, convenience, or, in a way — the *sense* of control, one gains through an electronic interaction.

The sharpening of the competitive edge to improve products and services now demands that businesses make sense of complex and voluminous data. This enables businesses to design effective sales campaigns, precision targeted marketing plans, and develop products to increase sales and profitability. In this context, a technology called "data mining" can be a valuable tool for business because it provides for the "efficient discovery of valuable, non-obvious information from a large collection of data."[2]

Although data mining can be extremely valuable for businesses, it can also, in the absence of adequate safeguards, jeopardize informational privacy. For this reason, the Office of the Information and Privacy Commissioner (IPC) has produced this report on data mining.

The report is aimed primarily at consumers and businesses. It covers the following: What is Data Mining; Examples of Data Mining; The Implications of Data Mining in the Context of Fair Information Practices; and Consumers and Businesses: Choices to Consider. (The "fair information practices" discussed refer to the basic principles of data protection first established in 1980 by the Organisation for Economic Co-operation and Development).

1 IBM, *Data Mining: Make your data work for you like never before*, at direct.boulder.ibm.com/bi/tech/mining/index.html. Viewed on July 7, 1997.

2 Joseph P. Bigus, *Data Mining with Neural Networks* (United States: McGraw-Hill, 1996), p. 9.

Generally speaking, we think that responsible data management in private sector businesses must be firmly based on fair information practices. The protection of personal information can be enhanced if: (1) consumers *choose* to voice and act on their expectations about the privacy of their personal information to the businesses with which they are transacting; and (2) businesses *choose* to adopt a culture of privacy through tangible everyday practices and through the use of privacy enhancing technologies. It comes down to a matter of choice for both consumers *and* for businesses.

Ultimately though, the IPC sees the need for government, businesses and consumers to share the responsibility in the management of the collection, use, retention and disclosure of personal information held by private sector businesses. We support a shared responsibility approach that is codified through government enactment of data protection legislation for private sector businesses, sustained by the business community adopting a culture of privacy; and strengthened by consumers taking greater control of their own personal information and voicing their privacy expectations to the business community.

Backdrop

The transformation of information storage from paper-based records to electronic formats has contributed to the mounting attention and concern about informational privacy in the marketplace.

Two examples illustrate this point: 1) Canadian surveys show that increasingly, people are concerned about their privacy and the prospect of being watched;[3] and, 2) *Time* magazine pronounced the "The Death of Privacy" (cover story Canadian edition, August 25, 1997).

While we believe that *Time's* pronouncement to be somewhat exaggerated, it is true that the information age now upon us is bringing with it recurrent horror stories about loss of privacy and *dataveillance*, the exploits of hackers and breaches of security, and identity theft — the impersonation and fraudulent use of your identity by another. Certainly the Internet and electronic commerce have heightened concerns over privacy and security issues that were unthought of previously:

> As we move toward a more fully digital world, the cost of manipulating information approaches zero, and the hazards therein multiply. Even our privacy is in peril. The "clickstream" pouring into Web merchants — the information that you provide with clicks of your mouse … what music you listen to and where you like to eat — lets those merchants personalize their marketing, but it may be more information than you want to share widely. And some Web entrepreneurs collect this information and sell it. Supermarket scancards may be more

3 For more information, see the following surveys: The Equifax Canada Report on *Consumers and Privacy in the Information Age* (1995); The Ekos Research Associates Inc. survey, *Privacy Revealed: The Canadian Privacy Survey* (1993); *The Information Highway: What Canadians Think about the Information Highway* (1994); and, *Surveying Boundaries: Canadians and Their Personal Information* (1996).

convenient than coupons, but … they, too, "put a price on privacy." The activities in these examples are perfectly legal, of course, but they increase the potential for electronic malfeasance.[4]

Within this environment of a booming information economy, bringing with it a new set of challenges to data protection, two noteworthy responses have emerged in Canada:

- The Canadian Standards Association (CSA) released its *Model Code for the Protection of Personal Information* (the Code) in March 1996 — this Code, although voluntary, provides a national standard for the protection of personal information in non-government organizations.

It is likely that the Code will form the foundation of any future data protection legislation in Canada covering the private sector. (Quebec is the only province in Canada that has legislation that sets out fair information practices for businesses operating in that province.)

- In September 1996, the Federal Government announced its commitment to the introduction of privacy legislation covering the private sector by the year 2000. Drafting of the bill is said to be underway.

"It has been estimated that the amount of information in the world doubles every 20 months, and the size and number of databases are increasing even faster."[5] Thus, it is with some sense of urgency that we have prepared this report on data mining with the view that, an entrenched culture of privacy in the business world will only come about if consumers speak up and convey their privacy expectations to businesses, and, if businesses truly believe that privacy protection makes good business sense.

What is Data Mining?

Data mining is a set of automated techniques used to extract buried or previously unknown pieces of information from large databases. Successful data mining makes it possible to unearth patterns and relationships, and then use this "new" information to make proactive knowledge-driven business decisions. Data mining then, "centres on the automated discovery of new facts and relationships in data. The raw material is the business data, and the data mining algorithm is the excavator, sifting through the vast quantities of raw data looking for the valuable nuggets of business information."[6]

Data mining is usually used for four main purposes: (1) to improve customer acquisition and retention; (2) to reduce fraud; (3) to identify internal inefficiencies and then revamp operations, and (4) to map the unexplored terrain of the Internet.[7] The primary

4 Marshall Jon Fisher, "moldovascam.com," *The Atlantic Monthly*, September 1997, p. 22.

5 Queen's University of Belfast, *What is Data Mining?*, at **www.pcc.qub.ac.uk/tec/courses/datamining/stu_notes/dm_book_2.html#HEADING2**. Viewed on July 4, 1997.

6 Bigus, *Data Mining with Neural Networks*, p. 9.

7 Nick Wreden, *Communications Week Interactive*, February 17, 1997, at **cmp-pub1.web.cerf.net/cw/cwi/pages/021797/650close.htm**. Viewed on August 11, 1997.

types of tools used in data mining are: neural networks, decision trees, rule induction, and data visualization.

Although not an essential prerequisite, data mining potential can be enhanced if the appropriate data have been collected and stored in a *data warehouse* — a system for storing and delivering massive quantities of data. "Data warehousing is the process of extracting and transforming operational data into informational data and loading it into a central data store or warehouse."[8]

The promise of data warehousing is that data from disparate databases can be consolidated and managed from one single database.

The link between data mining and data warehousing is explained as follows:

Data warehousing is the strategy of ensuring that the data used in an organization is available in a consistent and accurate form wherever it is needed. Often this involves the replication of the contents of departmental computers in a centralized site, where it can be ensured that common data definitions are in the departmental computers in a centralized site, where it can be ensured that the common data definitions are in use…

The reason data warehousing is closely connected with data mining is that when data about the organization's processes becomes readily available, it becomes easy and therefore economic[al] to mine it for new and profitable relationships.[9]

Thus, data warehousing introduces greater efficiencies to the data mining exercise. "Without the pool of validated and scrubbed data that a data warehouse provides, the data mining process requires considerable additional effort to pre-process the data."[10] Notwithstanding, it is also possible for companies to obtain data from other sources via the Internet, mine the data, and then convey the findings and new relationships internally within the company via an Intranet.[11]

There are four stages in the data warehousing process:

> The first stage is the acquisition of data from multiple internal and external sources and platforms. The second stage is the management of the acquired data in a central, integrated repository. Stage three is the provision of flexible access, reporting and analysis tools to interpret selected data. Finally, stage four is the production of timely and accurate corporate reports to support managerial and decision-making processes.[12]

8 Queen's University of Belfast, *What is Data Mining?*

9 Michael Bell, *A Data Mining FAQ*, at **www.qwhy.com/dmfaq.htm**. Viewed on August 26, 1997.

10 SAS Institute, *What is Data Mining?*, at **www.sas.com/feature/4qdm/whatisdm.html**. Viewed on July 25, 1997.

11 Ibid.

12 Conspectus, *The Data Warehousing Boom*, at **www.pmp.co.uk/feb2.htm**. Viewed on July 24, 1997.

Though the term data mining is relatively new, the technology is not. Many of the techniques used in data mining originated in the artificial intelligence research of the 80s and 90s. It is only more recently that these tools have been applied to large databases. Why then are data mining and data warehousing mushrooming now? IBM has identified six factors that have brought data mining to the attention of the business world:

1 A general recognition that there is untapped value in large databases;

2 A consolidation of database records tending toward a single customer view;

3 A consolidation of databases, including the concept of an information warehouse;

4 A reduction in the cost of data storage and processing, providing for the ability to collect and accumulate data;

5 Intense competition for a customer's attention in an increasingly saturated marketplace;

6 The movement toward the de-massification of business practices.[13]

With reference to point six above, "de-massification" is a term originated by Alvin Toffler. It refers to the shift from mass manufacturing, mass advertising and mass marketing that began during the industrial revolution, to customized manufacturing, advertising and marketing targeted to small segments of the population.

There are three basic steps in data mining:

> The first processing step is data preparation, often referred to as "scrubbing the data." Data is selected, cleansed, and preprocessed under the guidance and knowledge of a domain expert. Second, a data mining algorithm is used to process the prepared data, compressing and transforming it to make it easy to identify any latent valuable nuggets of information. The third phase is the data analysis phase where the data mining output is evaluated to see if additional domain knowledge was discovered and to determine the relative importance of the facts generated by the mining algorithms.[14]

Data mining differs from other analytical tools in the approach used in exploring the data relationships. Traditional database queries can answer questions like "what were my sales in Kenora in 1996?" Other analyses, often called multidimensional or online analytical processing, allow users to do more complex queries, such as comparing sales relative to plan by quarter and region for the prior two years.[15] In both cases, however, the results are simply figures extracted from the data or an aggregate of existing data. The relationship among these data is already known to the user, who, by framing the proper question, obtains the desired answer.

13 IBM, *Data Mining — An IBM Overview*, at **direct.boulder.ibm.com/bi/info/overview.htm**. Viewed on July 7, 1997.

14 Bigus, *Data Mining with Neural Networks*, pp. 10–11.

15 Herb Edelstein, "Mining Data Warehouses," *Information Week*, January 8, 1996, p. 48.

Data mining however, uses discovery-based approaches in which pattern-matching and other algorithms are used to discover key relationships in the data, previously unknown to the user.

> The discovery model is different because the system automatically discovers information hidden in the data — the data is sifted in search of frequently occurring patterns, trends, and generalisations about the data without intervention or guidance from the user… An example of such a model is a bank database which is mined to discover the many groups of customers to target for a mailing campaign. The data is searched with no hypothesis in mind other than for the system to group the customers according to the common characteristic found.[16]

Data mining usually yields five types of information — associations, sequences, classifications, clusters, and forecasting:

> Associations happen when occurrences are linked in a single event. For example, a study of supermarket baskets might reveal that when corn chips are purchased, 65% of the time cola is also purchased, unless there is a promotion, in which case cola is purchased 85% of the time.
>
> In sequences, events are linked over time. [For example][I]f a house is bought, then 45% of the time a new oven will be bought within one month and 60% of the time a new refrigerator will be bought within two weeks.
>
> Classification is probably the most common data mining activity today… Classification can help you discover the characteristics of customers who are likely to leave and provide[s] a model that can be used to predict who they are. It can also help you determine which kinds of promotions have been effective in keeping which types of customers, so that you spend only as much money as necessary to retain a customer.
>
> Using clustering, the data mining tool discovers different groupings with the data. This can be applied to problems as diverse as detecting defects in manufacturing or finding affinity groups for bank cards.
>
> All of these applications may involve predictions, such as whether a customer will renew a subscription … [f]orecasting, is a different form of prediction. It estimates the future value of continuous variables — like sales figures — based on patterns within the data.[17]

Generally then, applications of data mining can generate outputs such as:

16 Queen's University of Belfast, *What is Data Mining?*

17 Herb Edelstein, *Technology How To: Mining Data Warehouses*, at **techweb.cmp.com/iw/.561/61oldat.htm**. Viewed on July 24, 1997.

- Buying patterns of customers; associations among customer demographic characteristics; predictions on which customers will respond to which mailings;
- Patterns of fraudulent credit card usage; identities of "loyal" customers; credit card spending by customer groups; predictions of customers who are likely to change their credit card affiliation;
- Predictions on which customers will buy new insurance policies; behaviour patterns of risky customers; expectations of fraudulent behaviour;
- Characterizations of patient behaviour to predict frequency of office visits.

As indicated above, data mining applications can be used in a variety of sectors: retail, finance, manufacturing, health, insurance, and utilities. Therefore across all sectors — if a business has data about its customers, suppliers, products, or sales, it can benefit from data mining. It is expected that data mining will be one of the greatest tools to be used by the business community in the next century as its ability to capitalize on the use of an already existing resource — information — becomes widely recognized, and the cost of data mining software goes down.

With regard to customers, the types of data that are needed to perform data mining applications are: 1) demographics, such as age, gender and marital status; 2) economic status, such as salary, profession and household income; and, 3) geographic details, such as city, street, province, rural/urban. All of these data types can be used to delineate particular sets or segments of customers that share similar interests and have common product requirements.

Examples of Data Mining

It has been estimated that the data mining market will reach more than $800 million by the year 2000.[18] The Gartner Group predicted that by the end of 1997, approximately 80 per cent of the Global 2000 (the world's largest 2,000 companies) will have or will be planning a data warehouse strategy that will likely incorporate data mining.[19]

By the year 2000, at least half of the Fortune 1000 companies worldwide will be using data mining.[20] Not surprising, when you think of the potential benefits to the businesses using various applications. Take, for example, the ability to scour data from multiple databases to predict future trends and behaviours: Blockbuster Entertainment uses it to recommend video rentals to individual customers;[21] American Express uses it to suggest products to its cardholders based on an analysis of their monthly spending patterns.[22]

18 META Group, *Press Release on META Group Announces, "Data Mining Opportunities: 1996–1998*," at **www.metagroup.com/newweb.nsf/Web+Pages/OldPR**. Viewed on August 7, 1997.

19 Wreden, "The Mother Lode," *Communications Week Interactive*.

20 Kurt Thearling — The Data Intelligence Group, *From Data Mining to Database Marketing*, at **www.santafe.edu/~kurt/wp9502.shtml**. Viewed on August 7, 1997.

21 Author unknown, *Data Mining: What is Data Mining?*, at **www.anderson.ucla**. Viewed on July 25, 1997.

22 Ibid.

MasterCard International uses it to extract statistics about its millions of daily cardholder transactions; furthermore, MasterCard plans to sell "a data warehouse of those transactions to its 20,000 business partners — banks and other companies, such as Shell Oil, that offer credit-card services."[23]

The Internet is also becoming an emerging frontier for data mining. Some technology companies provide "virtual" data mining services via the Internet. With access to an Internet server, it is possible to FTP (file transfer protocol) the data from the client's server and then conduct various data mining activities. (Alternately, if the client does not have access to an Internet server or if the data are too sensitive or voluminous, the data mining services can occur when the client provides a computer tape).[24]

Internet websites can be a further source of data for companies who want to know more about visitors to their own websites. For example:

> The Chicago Tribune Co. publishes a variety of services on the Web and on America Online Inc, … many of which are focused on classified marketing. The Chicago Tribune uses data mining to analyze customer behaviour as they move through its various sites.[25]

WalMart is often described as a pioneering leader in data mining and data management:

> WalMart captures point-of-sale transactions from over 2,900 stores in six countries and continuously transmits this data to its massive 7.5 terabyte data warehouse. WalMart allows more than 3,500 suppliers to access data on their products and perform data analyses. These suppliers use this data to identify customer buying patterns at the store display level. They use this information to manage local store inventory and identify new merchandising opportunities.[26]

Other companies supplement their customers' transactional information with external data such as postal codes to do a market basket analysis:

> Practically every retailer now records all the details of each POS (Point of Sale) transaction for stock keeping purposes. Sometimes these are supplemented by customer information. Home Depot, for example, supplements the data with ZIP or postal code of the purchaser. Sometimes the cashier may also enter the sex and appropriate age of the customer into the cash register. Affinity cards and credit card numbers can be used to track repeat customers. Market Basket Analysis is the analysis of the data that this generates with a view to improving the performance of the retail outlet.[27]

23 Barbara DePompa, "There's Gold in the Databases," *Information Week*, January 8, 1996, p. 54.

24 One reference is **www.ultragem.com/ultrafaq.htm#howquestion**. Viewed on July 4, 1997.

25 Wreden, "The Mother Lode," *Communications Week Interactive*.

26 Author unknown, *Data Mining: What is Data Mining?*

27 Bell, *A Data Mining FAQ.*

Another example of what data mining can do involves the directed targeting of customers for new products, at a fraction of the cost:

> A credit card company can leverage its vast warehouse of customer transaction data to identify customers most likely to be interested in a new credit product. Using a small test mailing, the attributes of customers with an affinity for the product can be identified. Recent projects have indicated more than a 20-fold decrease in costs for targeted mailing campaigns over conventional approaches.[28]

In the health care field, data mining applications are growing quickly. Applications can be used to directly assist practitioners in improving the care of patients by determining optimal treatments for a range of health conditions. Data mining is used to assist caregivers to distinguish patients who are statistically at risk for certain health problems so that those patients can be treated before their conditions worsen. Data mining can also be used to detect possible fraudulent behaviours of health providers as well as health service claimants. For example, patterns of care indicating that a particular practitioner is ordering too many diagnostic tests or conducting tests that are inappropriate may be identified through data mining; similarly, patterns, associations and overpayments for claims made by patients can be discovered through this process.

As much of the literature suggests, however, data mining is not a magic bullet nor a simple process. It also presents challenges that go well beyond the technical:

> Many data management challenges remain, both technical and societal. Large online databases raise serious societal issues. To cite a few of the societal issues: Electronic data interchange and data mining software make it relatively easy for a large organization to track all of your financial transactions. By doing that, someone can build a very detailed profile of your interests, travel, and finances. Is this an invasion of your privacy? Indeed, it is possible to do this for almost everyone in the developed world. What are the implications of that?[29]

In the next section we will explore the implications of data mining in the context of a set of principles designed to protect and guide the uses of personal information, commonly referred to as "fair information practices."

The Implications of Data Mining in the Context of Fair Information Practices

Around the world, virtually all privacy legislation, and the policies, guidelines, or codes of conduct used by non-government organizations, have been derived from the set of principles established in 1980 by the Organisation for Economic Co-operation and Development (OECD). These principles are often referred to as "fair information

28 Pilot Software, *Data Mining White Paper — Profitable Applications* found at, **www.pilotsw.com/dmpaper/dmindex.htm#dmapp**. Viewed on July 4, 1997.

29 Jim Gray, Data Management: Past, Present, and Future, at **www.research.microsoft.com/%7Egray/DB_History.htm**. Viewed on August 12, 1997.

practices," and cover eight specific areas of data protection (or informational privacy). These are: (1) Collection Limitation; (2) Data Quality; (3) Purpose Specification; (4) Use Limitation; (5) Security Safeguards; (6) Openness; (7) Individual Participation; and (8) Accountability.

Essentially, these eight principles of data protection or fair information practices codify how personal data should be protected. At the core of these principles is the concept of personal control — the ability of an individual to maintain some degree of control over the use and dissemination of his or her personal information.

Concerns about informational privacy generally relate to the manner in which personal information is collected, used and disclosed. When a business collects information without the knowledge or consent of the individual to whom the information relates, or uses that information in ways that are not known to the individual, or discloses the information without the consent of the individual, informational privacy may be violated.

Data mining is a growing business activity, but from the perspective of fair information practices, is privacy in jeopardy? To determine this, we reviewed data mining from a fair information practices perspective. As discussed below, we have identified issues with five of these principles.

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 up-to-date.

Any form of data analysis is only as good as the data itself. Data mining operations involve the use of massive amounts of data from a variety of sources: these data could have originated from old, current, accurate or inaccurate, internal or external sources. Not only should the data be accurate, but the accuracy of the data is also dependent on the input accuracy (data entry), and the steps taken (if in fact taken), to ensure that the data being analyzed are indeed "clean."

This requires a data mining operation to use a good data cleansing process to clean or scrub the data before mining explorations are executed. Otherwise, information will be inaccurate, incomplete or missing. If data are not properly cleansed, errors, inaccuracies and omissions will continue to intensify with subsequent applications. Above all else, consumers will not be in a position to request access to the data or make corrections, erasures or deletions, if, in the first instance, the data mining activities are not known to them.

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.

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.

Purpose Specification means that the type of personal data an organization is permitted to collect is limited by the purpose of the collection. The basic rule is that data collected should be relevant and sufficient, but not excessive for the stated purpose. In other words, restraint should be exercised when personal data are collected. *Use Limitation* means that the purpose specified to the data subject (in this case, the consumer) at the time of the collection restricts the use of the information collected. Hence, the information collected may only be used for the specified purpose unless the data subject has provided consent for additional uses.

Data mining techniques allow information collected for one purpose to be used for other, secondary purposes. For example, if the primary purpose of the collection of transactional information is to permit a payment to be made for credit card purposes, then using the information for other purposes, such as data mining, without having identified this purpose before or at the time of the collection, is in violation of both of the above principles. The primary purpose of the collection must be clearly understood by the consumer and identified at the time of the collection. Data mining, however, is a secondary, future use. As such, it requires the explicit consent of the data subject or consumer.

The *Use Limitation Principle* is perhaps the most difficult to address in the context of data mining or, indeed, a host of other applications that benefit from the subsequent use of data in ways never contemplated or anticipated at the time of the initial collection. Restricting the secondary uses of information will probably become the thorniest of the fair information practices to administer, for essentially one reason: at the time these principles were first developed (in the late 70s), the means by which to capitalize on the benefits and efficiencies of multiple uses of data were neither widely available nor inexpensive, thus facilitating the old "silo" approach to the storage and segregated use of information.

With the advent of high speed computers, local area networks, powerful software techniques, massive information storage and analysis capabilities, neural networks, parallel processing, and the explosive use of the Internet, a new world is emerging. Change is now the norm, not the exception, and in the quickly evolving field of information technology, information practices must also keep pace, or run the risk of facing extinction. Take, for example, the new directions being taken intending to replace the information "silos" of old, with new concepts such as "data integration" and "data clustering." If privacy advocates do not keep pace with these new developments, it will become increasingly difficult to advance options and solutions that can effectively balance privacy interests *and* new technology applications. Keeping pace will enable us to continue as players in this important arena, allowing us to engage in a meaningful dialogue on privacy and future information practices.

The challenge facing privacy advocates is to address these changes directly while preserving some semblance of *meaningful* data protection. For example, in the context of data mining, businesses could easily address this issue by adding the words "data mining" as a primary purpose at the time of data collection — but would this truly constitute "meaningful" data protection? Take another example: when applying for a new credit card, data mining could be added to the purposes for which the personal information collected on the application form would be used. But again, would this type of general, catch-all purpose be better than having no purpose at all? Possibly, but only marginally so.

The quandary we face with data mining is what suggestions to offer businesses that could truly serve as a meaningful primary purpose. The reason for this lies in the very fact that, at its essence, a "good" data mining program cannot, in advance, delineate what the primary purpose will be — its job is to sift through all the information available to unearth the unknown. Data mining is predicated on finding the unknown. The discovery model upon which it builds has no hypothesis — this is precisely what differentiates it from traditional forms of analysis. And with the falling cost of memory, the rising practice of data warehousing, and greatly enhanced processing speeds, the trend toward data mining will only increase.

The data miner does not know, cannot know, at the outset, what personal data will be of value or what relationships will emerge. Therefore, identifying a primary purpose at the beginning of the process, and then restricting one's use of the data to that purpose are the antithesis of a data mining exercise.

This presents a serious dilemma for privacy advocates, consumers, and businesses grappling with the privacy concerns embodied in an activity such as data mining. To summarize, the challenge lies in attempting to identify as a primary purpose, an as yet, unknown, secondary use. We offer some suggestions on how to address this issue in the next section.

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.

The principle of openness or transparency refers to the concept that people have the right to know what data about them have been collected, who has access to that data, and how the data are being used. Simply put, it means that people must be made aware of the conditions under which their information is being kept and used.

Data mining is not an open and transparent activity. It is invisible. Data mining technology makes it possible to analyze huge amounts of information about individuals — their buying habits, preferences, and whereabouts, at any point in time, without their knowledge or consent. Even consumers with a heightened sense of privacy about the

use and circulation of their personal information would have no idea that the information they provided for the rental of a movie or a credit card transaction could be mined and a detailed profile of their preferences developed.

In order for the process to become open and transparent, consumers need to know that their personal information is being used in data mining activities. It is not reasonable to expect that the average consumer would be aware of data mining technologies. If consumers were made aware of data mining applications, then they could inquire about information assembled or compiled about them from the business with which they were transacting — "information" meaning inferences, profiles and conclusions drawn or extracted from data mining practices.

Ultimately, openness and transparency engender an environment for consumers to act on their own behalf (should they so choose). Consumers could then make known to the businesses they were transacting with, their expectations about the collection, re-use, sale and resale of their personal information.

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; b) to have communicated to him, data relating to him i) within a reasonable time, ii) at a charge if any that is not excessive, iii) in a reasonable manner and iv) in a form that is readily intelligible to him; c) to be given reasons if a request made under subparagraph (a) and (b) is denied, and to be able to challenge such denial; and d) to challenge data relating to him and, if the challenge is successful, to have the data erased, rectified, completed or amended.

Data mining operations are extremely far removed from the point of transaction or the point of the collection of the personal information. As data mining is not openly apparent to the consumer, then the consumer is not aware of the existence of information gained through a data mining application. This prevents any opportunity to: 1) request access to the information, or 2) challenge the data and request that corrections, additions, or deletions be made.

Consumers and Businesses — Choices to Consider

Consumers

In the United States, media coverage of public concerns about informational privacy matters began around the start of this decade with the uproar that erupted over *Lotus Marketplace: Households*.[30] This was an early and perhaps defining demonstration of the public's sensitivity about informational privacy. In 1996, the Lexis-Nexis incident

30 *Lotus Marketplace: Households* was a series of disks produced by Equifax and Lotus Development Corporation in 1990. On these disks (available to anyone for a price), were the names, addresses, buying habits and income information of roughly 120 million American consumers. Over 30,000 consumer enquiries and complaints lodged shortly after its release effectively cancelled the sale of the disks.

drew massive attention to how people feel about their personal information: LexisNexis, an online information service in Dayton, Ohio, was accused of making social security numbers and other personal information widely available in its P-TRAK locator service. Then in 1997, after an electronic firestorm, America Online backed off of its plan to rent out its subscribers' telephone numbers.[31] In each of these cases, businesses quickly responded to a public outcry from their customers and either withdrew their products or changed their policies.

However, in order for consumers to react (and businesses to respond), consumers must have knowledge and awareness that something they could potentially choose to object to is actually occurring. The invisible nature of data mining (to the consumer) eliminates this possibility. In order for data mining to fall into line with fair information practices, the first step for consumers must be an awareness that any large business they are transacting with could be carrying out data mining activities. For some consumers, this knowledge will make no difference; for others, it will matter a great deal.

Once consumers are equipped with knowledge, it is up to each individual to decide for him or herself what matters, and based on that, what choices they want to make about assuming control over the uses of their personal information.

Concerned consumers *can* choose to take responsibility by informing businesses of their requirements and expectations regarding privacy. To assist in framing privacy-related questions relating to data mining, consumers may wish to consider the questions below. Then it is up to the consumer to decide what course of action, if any, to take.

As a consumer:

- Do you expect to be informed of any additional purposes that your personal information may be used, beyond the primary purpose of the transaction?
- Do you expect the option to say "no" to secondary or additional uses of your personal information, usually provided in the form of opting-out of permitting the use of your personal information for additional, secondary uses? Or, do you expect an opportunity to "opt-in" to secondary uses?
- Do you expect a process to be in place that gives you the right to access any information a business has about you, at any point in time?
- Do you expect a process that permits you to challenge, and if successful, correct or amend any information held by a business about you, at any point in time?
- Do you expect an option to have your personal information anonymized for data mining purposes and/or, an option to conduct your transactions anonymously?

For those consumers who wish to have greater control over the use and circulation of their personal information, we suggest the following initiatives:

31 Robert Ellis Smith, "Rapid-Response Time," *Privacy Journal*, August 1997, p. 1.

- Ask to see a business's privacy or confidentiality policy. Assess it against your expectations of how you want your personal information handled. If the policy does not meet your expectations, contact the business and inform it of your expectations. If no policy exists, inform the business that you expect respectful and fair handling of your personal information.
- Give only the minimum amount of personal information needed to complete a transaction.

If you are in doubt about the relevance of any information that is requested, ask questions about why it is needed, and ask that all of the uses of the requested information be identified.

Businesses

Businesses need a corporate will to adopt a culture of privacy — piece-meal or theoretical approaches will not be effective in responding to consumers' concerns. Ultimately, the impact of various technologies on privacy, including data mining, can only be averted by instilling a culture of privacy within the organization.

"Instilling a culture of privacy" means that businesses will have to tackle the conflict between the "use limitation" principle and the secondary uses of personal information arising out of data mining. It may be advisable for businesses to provide a multiple choice opt-out selection whereby consumers are given three choices: the choice of not having their data mined at all; only having their data mined in-house; or having their data mined externally as well. (Studies have shown that less concern is expressed over the *internal* secondary uses of one's data by the company collecting the data, but far greater resistance to having data disclosed externally for use by unknown parties.)

Is your business willing to:

- Have a privacy strategy that is,
    - based on fair information practices and entrenched through tangible actions;
    - resourced throughout all facets of the organization; and
    - evaluated and assessed so that ongoing adjustments and improvements can be made?
- Have an open and transparent relationship with its customers?
    - Do you inform your customers upfront as to how all information collected about them will be used and disclosed, and by whom?
    - Do you have a process that makes it easy for customers to find out what personal information you have about them and a process to challenge any information that may be incorrect, incomplete, inaccurate or out-of-date?

- Accept that some consumers do not want their personal information to be mined, and nuggets about their buying patterns extracted?
    - Do you advise consumers of all uses of their personal information and give them a range of opt-out choices about data mining such as: 1) no data mining; 2) data mining internally; 3) data mining internally and externally. Or, for maximum choice and control, do you provide consumers with positive consent — an opportunity to "opt-in" for specified secondary uses of their personal information?
- Use privacy-enhancing technologies that can anonymize information and securely protect privacy?

Although there is no data protection legislation governing the collection, use and disclosure of personal information in the private sector (with the exception of Quebec), there are resources that can provide practical ways for businesses to address the protection of personal information. Some notable sources are the following:

- The Canadian Standards Association's *Model Code for the Protection of Personal Information (CAN/CSA-Q830-96)* and its companion publication, *Making the CSA Privacy Code Work for You — A workbook on applying the CSA Model Code for the Protection of Personal Information (CAN/CSA-Q830) to your organization*.
- The use of privacy-enhancing technologies such as blind signatures (which build on public key encryption) and biometric encryption. Each of these technologies relies on the "blinding" of identity through advance forms of encryption. Similarly, through the use of an anonymous database,[32] personal and identifying information may be encrypted and stored separately in different locations — enabling businesses to consolidate their databases and keep them secure, while protecting privacy at the same time.
- Previous publications of the IPC have also outlined a range of ways in which businesses can carry out responsible data management practices with respect to the impact of technology on consumers' personal information: *Privacy Protection Makes Good Business Sense* (October 1994); *Privacy and Electronic Identification in the Information Age* (November 1994); *Privacy-Enhancing Technologies: The Path to Anonymity, 2 Volumes* (August 1995); *Identity Theft* (June 1997), and *Smart, Optical and Other Advanced Cards: How to do a Privacy Assessment* (September 1997).

32 Mytec Technologies Inc., a Toronto-based company, has developed a system which permits the consolidation of various databases but which keeps personal information under specific controls accessible only to those with a need to know. Mytec calls this system the "Anonymous Database." In the Anonymous Database, an individual's private and identifying information are encrypted and stored separately in different locations. Mytec uses the information contained in the pattern of a person's fingerprint to code a number called a "Bioscrypt" which operates as the link between an individual's private information and identifying information. For further information, see **www.mytec.com/applic/#database**.

- Professor Roger Clarke's strategic approach to privacy and dataveillance as set out in *Privacy and Dataveillance, and Organisational Strategy*[33] — provides a framework that can be used by businesses to develop a culture of privacy.

A Final Word

The need for protecting and managing personal information has been likened to the management of natural resources:

> Personal information is a resource, exploited commercially but valued as an element of human dignity and enjoyment of one's private life. It is therefore to be protected and managed, not unlike the protection and management of other resources. As with early efforts to protect the environment in the absence of legislation, privacy protection currently relies on ancient common law principles that continue to adapt to new technological challenges to personal integrity, happiness and freedom. These principles have now found legislative expression in various statutes relating to environmental protection. Information, however, has some unique qualities in need of special regulatory and judicial attention.[34]

Looking ahead, consumers will not only want goods and services, but will increasingly want assurances that the information they provide to a business is, from a privacy perspective, protected. To deal with this need, a shared responsibility for the management of personal information will be essential, involving government, the business community and consumers.

Only through shared responsibility, sustained by the business community through a culture of privacy, and strengthened by the voice of consumers, can personal information become a protected, managed and valued resource. We hope that this report will give all three parties — consumers, businesses, and government — incentives for action towards protecting personal information in the marketplace.

Finally, we believe that the tension between technology and privacy can be minimized if privacy safeguards are made a key consideration upfront, rather than as an afterthought. Although current data mining practices are somewhat beyond the "upfront" stage, there is still time to ease this "tension" before applications become widely commonplace. One short term approach, as suggested earlier, may be for businesses to provide consumers with choices in the form of multiple selection opt-outs. To explore further solutions on how to address the "primary purpose" dilemma that data mining presents, we are committed to an open exchange. We invite those of you with any ideas as to how to resolve this issue to contact us — we would welcome your comments and encourage an open dialogue.

33 See Roger Clarke's paper *Privacy and Dataveillance, and Organizational Strategy*, at **www.anu.edu.au/people/Roger.Clarke/DV/PStrat.html**. Viewed on October 9, 1997. This paper presents a framework to guide businesses and governments towards adopting a strategic approach to privacy.

34 Ian Lawson, *Privacy and Free Enterprise: The Legal Protection of Personal Information In the Private Sector* (Ottawa: Public Interest Advocacy Centre, 1992), p. 442.

Identity Theft: Who's Using Your Name?

June 1997

Introduction

Your new credit card fails to arrive in the mail. Months later, creditors you never heard of are repeatedly calling you and demanding payment for merchandise you never bought. Your credit history has always been perfect, but you are now being denied financing due to several delinquencies appearing on your credit report. Could this really be happening? Unfortunately, it could, and it has, to thousands of victims of a crime known as "identity theft."

As part of its mandate, the Office of the Information and Privacy Commissioner/Ontario (IPC) researches and comments on matters and trends relating to the issue of privacy protection. Identity theft, a crime resulting from the misappropriation and abuse of personal information, is a growing societal problem that deserves our attention. This report will look at what identity theft is, how it occurs, why people should be concerned, and what consumers and organizations can do to minimize their chances of being victimized. In particular, technological ways of protecting one's personal information will be explored.

A key underlying theme throughout the paper will be the idea that identity theft could be significantly reduced if more organizations adopt and follow fair information practices.[1]

What is identity theft?

Identity theft involves acquiring key pieces of someone's identifying information in order to impersonate them and commit various crimes in that person's name. Besides basic information like name, address and telephone number, identity thieves look for social insurance numbers, driver's license numbers, credit card and/or bank account numbers, as well as bank cards, telephone calling cards, birth certificates or passports. This information enables the identity thief to commit numerous forms of fraud: to go on spending sprees under the victim's name, to take over the victim's financial accounts, open new accounts, divert the victim's financial mail to the thief's address, apply for loans, credit cards, social benefits, rent apartments, establish services with utility companies, and more.

Why should I care?

Every year, thousands of people are victimized by identity thieves who steal millions from banks, retailers, and other creditors. In the United States alone, banks lost up to

1 In 1980, the OECD (Organization for Economic Co-operation and Development)developed a set of internationally-recognized principles for the responsible treatment of personal information commonly known as the Code of Fair Information Practices. The Code sets out several restrictions and standards concerning the collection, retention, use,disclosure and security of personal information. More recently, the Canadian Standards Association has developed an updated Code called the "Model Code for the Protection of Personal Information."

OECD *Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data*, September 1980.

Canadian Standards Association, CAN/CSA-Q830-96 *Model Code for the Protection of Personal Information*. A National Standard of Canada. March 1996.

2 U.S. Public Interest Research Group, *Theft of Identity: The Consumer X-Files*, August1996, pp. 14-15.

$90 million due to theft of identity in 1995.[2] Ultimately, every one of us must pay in the form of higher interest rates and service fees. U.S. officials are now describing identity theft as "the fastest growing crime in the nation," having identified it as "the leading form of consumer fraud."[3]

The theft of your identity can leave you with a poor credit rating and a ruined reputation which may take months or even years to correct. Meanwhile, due to your seemingly dreadful credit history, you may be denied jobs, loans, cheque-writing privileges, or the right to rent or buy accommodation. You may even risk false arrest and having your story viewed with suspicion.

A typical victim's financial losses alone due to identity theft have been calculated to be as high as $36,000. This includes telephone calls, notarized statements, loans, counselling fees, and lost wages resulting from time taken off work to deal with the problem. The figure does not include losses associated with paying off the thief's bills or being denied employment.[4]

On top of it all, victims are often surprised by the lack of co-operation from those they turn to for help. Police have at times denied that they are real victims and have even arrested them for the thief's crimes. Creditors and credit bureaus have accused victims of lying and dodging debts that they themselves had incurred. Credit bureaus have refused to remove false data from victims' records. In other words, if your identity gets stolen, you may essentially be left on your own to sort out the mess.

To make matters worse, many identity thieves are never caught, leaving them open to repeat this form of fraud again and again. What is really frightening, however, is how easy it is to steal someone's identity.

How can my identity get stolen?

Today's identity thieves are absconding with people's identifying data in much more sophisticated ways than through stolen wallets.[5] Some of these include:

- lurking around automatic teller machines (ATMs) and phone booths in order to capture PIN numbers (by watching through binoculars as the numbers are being entered, or more simply, by casting a watchful gaze over someone's shoulder). Travellers are a particularly favourite target;
- stealing mail from mailboxes or re-directing mail in an effort to collect credit cards, bank statements, credit card statements, pre-approved credit offers, tax information or other personal data. *Privacy Journal* has also pointed out "how automated credit bureaus freely accept an address change without confirming it or notifying the

3 Ibid., p. 14.
"Scam Artists Await Unwary Travellers," *Toronto Star*, December 2, 1995, p. F19.

4 U.S. Public Interest Research Group, *Theft of Identity: The Consumer X-Files*, August1996, pp. 15-16.

5 U.S. Public Interest Research Group, *Theft of Identity: The Consumer X-Files*, August1996.
Privacy Rights Clearinghouse, "Coping With Identity Theft: What to Do When an Imposter Strikes," Fact Sheet No. 17, May 1995.

consumer who is the subject of the file. An imposter can easily have a retail store enter a change of address for a consumer whose identity the imposter has misappropriated, and that is what thousands of credit fraud perpetrators are doing …;"[6]

- illegally obtaining personal credit reports;
- setting up telemarketing schemes to elicit account numbers from unsuspecting consumers;
- accessing personal information accidentally sent to the wrong fax number, e-mail address or voice mailbox;
- scavenging through the garbage in search of credit card or loan applications, employer's files, and identification/authentication data such as login IDs and passwords. Similarly, thieves can search erased disks for any retrievable data;
- sending false messages on the Internet (spoofing) in an effort to collect private information. For example, posing as travel agents or other service providers, identity thieves can make off with your credit card number once it has been entered to purchase a ticket or service;
- sending e-mail using someone else's computer or e-mail address;[7]
- using various software programs such as "signals analysis" and "sniffer" programs to intercept financial data, passwords, addresses or other personal information being sent over networks;
- breaking into computer systems and gaining access to personal data. For example, names, addresses and credit card or social insurance/security numbers (SINs/SSNs) located in the databases of governments, financial organizations, employers, creditors, and credit bureaus can be downloaded by employees, former employees or external hackers. They can then sell the information or use it to open fraudulent accounts.

One security expert found that nearly 70 per cent of the websites he surveyed in December1996 had "security lapses." Surveyed sites included banks, credit unions and government agencies.[8] Even more recently, a 14-year-old boy faced multiple charges after making $3,000 worth of fraudulent purchases using a collection of debit card numbers that he had downloaded from the Internet.[9]

Identity theft case files

To provide readers with some understanding of the stress and aggravation that identity theft victims must endure, this section will outline several actual cases.

6 "Fraud Happens: Here's How," *Privacy Journal*, July 1996, pp. 5-6.

7 Marta Gold, "Easy E-mail Easy to Open — PC Privacy Just an Illusion," *Southam Newspapers*, February 15, 1997.

8 "Web Security Studied," *Globe & Mail,* January 1, 1997, p. B6.

9 "Cops Bust Kid Who Found Credit Numbers on 'Net' Site," *Privacy Times*, January 16,997, p. 3.

- A young secretary spent years trying to clear her name after a tax evader got hold of her SIN card, which the secretary had never received. The imposter used the secretary's name and SIN to move from job to job and collect unemployment insurance, health benefits, and maternity benefits — all without paying any taxes. The secretary was continually harassed by the government to settle "her" unpaid income taxes. Revenue Canada even garnisheed her bank account and earnings. The victim had to travel to each of the thief's six former employers, pleading for written statements to prove to tax officials that she herself had never worked there.[10]

- Using someone else's birth certificate and SIN card, a Vancouver man managed to obtain a photo ID card from the British Columbia government. He later used these three pieces of identification to open fraudulent bank accounts. He then proceeded to steal over $170,000 from several banks. This was done primarily by depositing bogus cheques into the accounts and immediately withdrawing the money through ATMs.[11]

- A Parisian woman whose ID card had been stolen, later found records indicating, much to her surprise, that she had been "married" for four years to a man she had never met. Once her "husband" had obtained French citizenship, he divorced her.[12]

- In a multi-victim fraud case, a teacher opened fraudulent credit card accounts and stole $43,000 worth of merchandise using the names and SSNs of his students and colleagues. The thief took the personal information from a class list and from pay stubs stolen out of campus mailboxes. The victims had to persuade the three national credit bureaus to delete the fraudulent data from their credit reports permanently. They also asked that creditors be alerted not to extend credit in their names unless they first confirmed that the victims themselves were the ones opening the accounts.[13]

- When a disabled telecommuter received her credit report from TRW,[14] it was seven pages long and had over 15 past due fraudulent accounts. There was also a judgment against her from an eviction that had taken place from an apartment. Later, she also received notice that she had defaulted on a loan. When she went to file criminal charges against her identity thief, the local sheriff's department said that the case would probably never be looked at because there were only two detectives and "it was not as important as a murder." TRW required that she prove to the 15 creditors herself that she had filed a criminal report by sending them notarized

10 Geoff Baker, "Imposter Makes Life Hell for Secretary," *The Gazette (Montreal)*, November 5, 1992, p. A1.

11 Bob Stall, "He Conned His Way Into Hearts," *The Province (Vancouver)*, November 5,1995, p. A8.

12 "Marriage Was Surprise to Her: Wed 4 Years to Unknown Man," The Province(Vancouver), November 10, 1995, p. A43.

13 "'Theft of Identity' Rises to Thousands a Day," *Privacy Journal*, February 1996, pp. 1, 4.

14 TRW is one of the three major American credit bureaux (Equifax and Trans Union are the other two). TRW changed its name to Experian in the summer of 1996. See Robert Ellis Smith, "Privacy: The Untold Stories," *Wired*, February 1997, p. 96.

statements (at a cost of $10 each). None of the creditors prosecuted the thief, however, because they said it was not financially worthwhile to do so.[15]

- A year after her SSN was stolen, a former Californian was denied a mortgage because of numerous delinquent accounts appearing on her credit reports. After months of struggle, she succeeded in getting TRW to delete the false entries, only to see them reappear half a year later. Both Equifax and Trans Union misplaced her files and failed to remove as many as nine of the original 12 false entries. Adding insult to injury, Trans Union even hinted that the victim herself was the perpetrator.

  The victim's bad credit report also affected her husband, whose Visa card was consequently not renewed. She ended up suing the three credit bureaus for their abusive practices, testifying in court that creditors were calling her "at all hours of the day and night," and did not stop doing so until she moved to another state. Trans Union argued that systemic improvements to ensure maximum accuracy were costly and that credit bureaus had no way to differentiate between genuine victims and consumers who themselves were committing fraud.[16]

- After years of turmoil, a Texas couple won a $1.45 million lawsuit against their identity thief for invasion of privacy, defamation, and a host of other charges. However, given the offender's paltry assets, this may have been a hollow victory. The offender was a former loans officer who had obtained the couple's personal information by using the bank's credit terminal to access their credit report. Using their SSNs, address, and financial account information, the thief opened 21 finance, gas and other credit accounts totalling approximately $50,000. In a separate action, the couple also sued 13 credit bureaus, collection agencies, banks, stores and other creditors involved in the case, for violations of privacy, defamation, and other charges.[17]

- After her military security clearance was suddenly suspended, an army employee discovered that a relative had stolen her identity and opened several fraudulent accounts. In an effort to clear herself, she paid off $30,000 in fraudulent debts. She then quit her job to go to a new one paying $30,000 a year, but the offer was subsequently withdrawn after the prospective new employer saw her credit report. As a result, she was left jobless and unable to hold on to her apartment. She was also unable to obtain any sort of government assistance or financial assistance from the credit bureaus involved. Ultimately, she had to leave the country because the only employment she was able to secure was in Korea.[18]

15 U.S. Public Interest Research Group, *Theft of Identity: The Consumer X-Files*, August1996, pp. 3-5.

16 "Going Against All Three," *Privacy Journal*, May 1996, pp. 4-5.
"L.A. Jury Identifies With 'Theft of Identity' Victim," *Privacy Journal,* August 1996,pp. 1, 4.

17 "Biggest Yet! Texas Couple Wins $1.45 Million for 'ID Theft'," *Privacy Times*, October5, 1995, pp. 1-3.

18 The Consumer X -Files pp. 6-7

- From an organization perspective, in a 1994 case, more than $300,000 was stolen from financial institutions using signatures and other personal information extracted from bank dumpsters. It has also been found that most credit report database intrusions maybe traced back to authorized terminals, not external hackers.[19]

Don't be an easy target

Personal information is now so readily available in the networked world we live in that it maybe impossible to eliminate identity theft entirely. Broader systemic and legislative reforms and the co-operative efforts of many including creditors, credit bureaus, law enforcement agencies and government, will be essential to combat the problem. In the meantime, however, there are several preventative measures that one can take, which may help to reduce one's chances of becoming a victim.[20] These are discussed in the sections that follow.

Low-tech methods

- Always store cards and documents containing sensitive personal data in a secure place. Sensitive data may include: credit cards, social insurance number, driver's license, bank account numbers, pre-approved credit applications, address, date of birth, tax records, passports, utility and phone bills. Shred (or tear up) all such documents prior to their disposal. Consider installing a secure mailbox.

- Obtain a copy of your credit report regularly to check for fraudulent accounts, false address changes and other fraudulent information. Report all errors to the credit bureau and have them immediately corrected.

- Keep and carry as few cards as possible. After completing a credit card transaction, make sure that the card you get back is your own. Tear up the carbon copies. Cancel all unused credit accounts.

- Carefully review all bank and credit card statements, cancelled cheques, phone and utility bills, as soon as you get them. Report any discrepancies immediately. If any regularly expected statements do not arrive on time, contact both the post office and your creditors to ensure that your mail isn't being diverted to another location.

- If you applied for a new credit card and it hasn't arrived on time, call the bank or credit card company involved. Report all lost or stolen cards right away.

19 "Flap Forces Connecticut Banks to Review Data Security Policies," *Privacy Times*, July20, 1995, p. 2.
U.S. Public Interest Research Group, *Theft of Identity: The Consumer X-Files*, August1996, p. 31.

20 Privacy Rights Clearinghouse, "Coping With Identity Theft: What to Do When an Imposter Strikes," Fact Sheet No. 17, May 1995.
Privacy Rights Clearinghouse, "What to Do When Your Wallet is Stolen," Fact Sheet No.13, June 1994.
PIRG Consumer Watchdog Fact Sheet: "What Can Consumers Do to Avoid Becoming Theft of Identity Victims?"

- Do not provide your address in conjunction with the use of your credit card. Your cheques should not have your driver's license preprinted on them. Also, avoid, unless legally required, writing your credit card number or SIN/SSN on your cheques.
- Avoid giving out your credit card number or other personal information over the telephone unless you have a trusted business relationship with the company and you have initiated the call. In particular, do not provide personal information over unencrypted wireless communications such as cordless or cellular phones. (Even baby monitors can broadcast your personal communications to eavesdroppers).
- Some card issuers call customers if they notice unusual charges on their cards. You should never give out any information about your account over the telephone except your confirmation of what has already occurred. If you have any doubts, hang up and contact the card issuer directly. Similarly, do not provide any personal information to unfamiliar callers claiming to be from your financial institution or brokerage firm. Ask for the person's name, hang up, and then call them back.[21]
- PINs and passwords should never be written down or revealed to anyone. Choose ones that cannot be easily guessed, and change them regularly. When conducting banking or investment transactions over the telephone, make sure that no one can hear you or be in a position to detect your PIN or password as it is being entered.
- If you should discover that your personal information has been placed in an online directory or a searchable database, try to have it removed. For example, one major U.S.database company has been selling names, addresses, birth dates, unlisted phone numbers and other data on millions of people over the Internet. Even SSNs were initially being offered until hundreds of people complained.[22]
- Do not create online profiles containing your personal information — it could be used by someone else to impersonate you.
- Beware of start-up software that asks for registration information including your credit card number and SIN/SSN, to upload "for billing purposes."

High-tech privacy-enhancing technologies

The world's expanding electronic infrastructure has enabled fraud to flourish exponentially. In our increasingly technology-driven world, the use of privacy-enhancing technologies can be a critical complement to the safe information practices outlined above. Privacy-enhancing technologies, or "PETs" refer to technologies that transmit your

21 Royal Bank Consumer Information brochure: "Straight Talk About Safeguarding Against Financial Fraud."
An impersonator can also cause problems by sending you a false message using someone else's e-mail address. It is a good idea to confirm e-mails with a reply to ensure that they are genuine.

22 "SSNs For Sale On-Line," *Privacy Journal*, June 1996, p. 4.
"Lexis-Nexis Spin: Did it Work?" *Privacy Journal,* September 1996, p. 7.

personal information in encrypted form, or otherwise enable you to conduct electronic transactions in an anonymous manner by minimizing or eliminating the collection of personally identifying data. Encryption is a mathematical process of encoding information so that it cannot be read without possession of the correct "key" necessary to decode it.

When transmitting information via a communications network, you should assume that your communications are not private, unless that information is encrypted.[23] Without strong encryption, Personal Computer (PC) banking, online investing, online shopping, sending and receiving e-mails, and processing commercial or credit applications over the Internet can expose personal information to unauthorized disclosure, theft and alteration.

The most rapidly increasing area for the commission of identity theft is said to be on the Internet.[24] This should not be surprising in light of the opportunities the Net provides for the collection (and abuse) of personal information, on a scale not previously possible. It has been predicted that by the year 2000, 30% of all North American commerce will take place in cyberspace, and worldwide Internet commerce revenues could reach $200 billion U.S.[25] With this will come ever-growing opportunities for identity theft.

A wide variety of PETs are available today. The following section will discuss some of the key ones. Combining additional security features with PETs, such as passwords and encryption, will further increase security and privacy.

Identity protectors

Identity protectors, such as blind signatures and digital pseudonyms, are mathematical sequences based on encryption techniques that enable users to conduct electronic transactions in an anonymous manner, while at the same time, allowing the service provider to verify the user's authenticity and eligibility for benefits and services.

Digital signatures are the electronic equivalent of handwritten signatures. Like handwritten signatures, which are used to authenticate paper documents, digital signatures placed on electronic documents serve the same purpose. Digital signatures can protect against spoofing and message forgeries, but they offer little privacy since they are intended to identify the originating party. **"Blind" signatures**, developed by David Chaum of DigiCash,[26] go one step further and provide the same authentication as digital signatures, but do so without revealing the originator's identity, thus rendering it "blind." The advantage of such a system is that it preserves the authenticating features of digital signatures, while protecting one's privacy at the same time.

23 Note that while encryption can significantly enhance security and privacy, it cannot guarantee it.

24 "Scam Artists Await Unwary Travellers," *Toronto Star*, December 2, 1995, p. F19.

25 Patrick Brethour, "Is This the Year for Internet Commerce?" *Globe & Mail,* January 15,1997, p. B12.

26 David Chaum: "Achieving Electronic Privacy," *Scientific American*, August 1992.

A digital pseudonym is an alternative pseudo-identity that a user may choose to assume in order to engage in a particular transaction, communication or service in an anonymous manner. One can select a different pseudonym for every service provider, or for use each time that a particular service is used.

For a more in-depth discussion on these and other PETs, readers may wish to see the joint report by the IPC and the Netherlands Data Protection Authority entitled, *Privacy-Enhancing Technologies: The Path to Anonymity*. Released in the fall of 1995, this paper provides a detailed analysis of advanced encryption techniques that allow for authenticated yet anonymous transactions, such as digital signatures, blind signatures, digital pseudonyms and trusted third parties.

Data encryption

Several powerful encryption programs are readily available at no charge through Internet service providers as stand-alone programs or as part of packages providing file or e-mail encryption and digital signatures. For example, one powerful public key encryption system, PGP, (Pretty Good Privacy) developed by Philip Zimmermann[27], may be used to encrypt e-mail or computer files.

An alternative to PGP is the Kerberos authentication scheme, which may be used to secure specific messages or to protect the server's protocol level. Privacy Enhanced Mail (PEM) may also be used to encrypt sensitive data before sending it over the Net.

Various technologies for encrypting credit card numbers for use in making payments over the Internet are now being developed, such as the Secure Electronic Transaction (SET) standard. Internet communications and transactions may also be encrypted using Secure Hypertext Transfer Protocol (S-HTTP) and Secure Sockets Layer (SSL).

Anonymous remailers

When you send a letter through the regular mail, you can remain anonymous simply by not putting your return address on the envelope. On the Net, however, your address is automatically forwarded, unless you take steps to channel your e-mail through an "anonymous remailer." An anonymous remailer is a free service that strips the identifying header from your e-mail before sending it on its way. For a range of anonymous services on the Net, take a look at: www.anonymizer.com.

Anonymous payment mechanisms

Electronic payments can take place anonymously through the use of smart cards such as stored-value cards, pre-paid transponders for electronic toll roads, or electronic cash involving digitally encoded money. Developed to serve as the electronic equivalent of cash, digital cash systems are designed so that transactions cannot be traced back to the purchaser, yet the payee is still assured of the payment's authenticity.

27 Steven Levy, "Crypto Rebels," *Wired*, May/June 1993.

Other PETs

- Computer security hardware and software, such as access control software and programs that prevent unauthorized online access to your computer, are available. Software that will turn an ordinary PC into a secure telephone can be downloaded from the Internet at no cost.

- Tokens are unique identification strings which may be stored on smart cards. Tokens may be used in combination with passwords/PINs, card readers, and at times, encryption.

- Special privacy-enhancing printers have mailboxes and collators with several locking trays, each of which can be assigned a password. Users can send their print jobs to their own secure output trays.

- Other PETs involve anonymous one-time signatures, protected passwords, one-time passwords, tiered levels of entry, partitioned access according to file sensitivity, and call blocking. One Internet service provider even offers free, anonymous Internet accounts, pseudonymous servers and "Anonymizer" services that allow users to surf the WorldWide Web "with complete anonymity."[28]

While privacy-enhancing technologies are available today, with new ones appearing on a regular basis, they are not yet widely known or used. Widespread implementation — throughout business, government and private industry — will only come about through consumer demand. By making yourself heard today, you can help to secure a more privacy-respectful electronic future for everyone.

What organizations can do

Organizations have an equal, if not larger role to play than consumers when it comes to preventing identity theft. *Privacy Times* reported that, "theft-of-identity cases are a direct response to criminals' increasing willingness to take advantage of inadequate security for personal financial data stored in credit bureaus and other large databases."[29] We make the following recommendations (especially applicable to financial and public sector organizations):

- When information systems are being designed or upgraded, consider how user-privacy could best be protected. Explore the application of PETs and ensure appropriate security measures are taken. Ask: How much personally identifiable information is actually required for this system to function? Once this has been determined, collect and retain only the minimum.

- Absent legislation, adopt a privacy policy for your organization and train all employees on responsible information handling practices. The Canadian Standards

28 Sandy Sandfort, "Making Privacy Pay," *Wired*, January 1997.

29 "Biggest Yet! Texas Couple Wins $1.45 Million for 'ID Theft'," *Privacy Times*, October5, 1995, p. 2.

Association's *Model Code for the Protection of Personal Information* (CAN/CSA Q830-96) is an excellent code for use by private sector organizations.

- Exercise considerable caution when collecting, using, and disclosing SINs/SSNs. Do not ask for these numbers if not required by law. Stolen SSNs result in thousands of cases of identity credit theft each month. Persons lacking proper documentation may steal these numbers in order to obtain legal identities. A SIN/SSN can also be used to impersonate someone over the telephone or online in order to retrieve personal data about the individual, such as tax information. Avoid the use of SINs/SSNs as client/employee/student identification numbers.
- Consider storing the textual portion of a record (i.e., clinical encounter data in a health record) separately without any personal identifiers; retain identifying information (such as name, SIN, address, date of birth) in a separate database, preferably in encrypted form. Organizations can also separate the flow of personal data from other transactional data in their information systems.
- If you are a credit bureau, provide your customers with a free credit report annually, upon request, and notify customers whenever their credit reports have been accessed.
- Require proof of identity and check it carefully when a customer applies for credit or a change of address. Credit bureaus should not accept client address changes from creditors without first verifying them with the consumer involved.
- Make use of artificial intelligence programs to identify patterns of fraudulent use and notify consumers of any suspected fraudulent activity. Creditors have a responsibility to report fraudulent accounts to the police and ensure that they are deleted from a bonafide client's record.
- Do not use customers' personal information for "secondary purposes" such as adding it to mailing lists or selling/leasing it to third parties, without the explicit consent of the individual concerned.
- Store and dispose of personal information accurately and securely, especially credit and loan application forms.
- Avoid using date of birth or mother's maiden name as passwords for financial accounts. This type of information is often quite easy for others to acquire.
- Do not put scanned copies of anyone's signatures on your organization's website.

30 PIRG Consumer Watchdog Fact Sheet: "A Checklist For Theft of Identity Victims."

Privacy Rights Clearinghouse, "Coping With Identity Theft: What to Do When an Imposter Strikes," Fact Sheet No. 17, May 1995.

31 For example, California's Privacy Rights Clearinghouse (619-298-3396) or Public Interest Research Group (310-397-3404).

What if it happens to me?

Identity theft is a multi-faceted problem that is unlikely to go away. If you should become a victim, you will need to take action quickly:[30]

- Notify the police, banks, and creditors immediately. Obtain a copy of your police report (as evidence of the fraud having been perpetrated). Cancel all existing credit cards, accounts, passwords and PINs, and replace them with entirely new ones.
- Call the credit bureaus and ask each to attach a fraud alert and victim's statement to your report. Ask creditors to call you prior to adding any new items to your report. Have all corrections forwarded to anyone who has received your credit report within the past two years. Ask for a free copy of your report after three months.
- Contact the post office if you suspect that an identity thief has filed a change of address form for your name, and is diverting your mail to another address.
- Alert all utility companies that someone has been using your identity fraudulently and inform the appropriate authorities that someone may be abusing your SIN and/or driver's license number.
- Take action to have any criminal or civil judgments against you that may have resulted from your identity thief's actions, permanently removed.
- Keep a log of all your contacts and make copies of all documents. You may also wish to contact a privacy or consumer advocacy group.[31]
- In some cases, it may be advisable to seek the assistance of a lawyer.

Conclusion

The theft of your identity can pose a serious threat to your privacy and has the potential to make your life very difficult. This paper has provided a brief look at some of the factors contributing to this crime, as well as possible ways of preventing it, and failing that, dealing with it.

The problem of identity theft must be fought on several fronts. Applying fair information practices is a good place to start. Moreover, as computers and networks make it easier and easier to gather your personal information, technological methods of protecting privacy will become increasingly important. Organizations that can offer their clients greater informational privacy may well obtain a competitive advantage over those who fail to do so. If enough people demand it, we may find that in the future, anonymous transactions (which authenticate identity in a blind manner), will become the standard, as opposed to the identifiable transactions of the present day. De-identifying information may well pave the way to a future which includes privacy.

Privacy-Enhancing Technologies: The Path to Anonymity (Volume 1)

August 1995

Introduction

At the present time, you are almost always required to reveal your identity when engaging in a wide range of activities. Every time you use a credit card, make a telephone call, pay your taxes, subscribe to a magazine, or buy something at the grocery store using a credit or debit card, an identifiable record of each transaction is created and recorded in a computer database somewhere. In order to obtain a service or make a purchase (using something other than cash), organizations require that you identify yourself. This practice is so widespread that it is simply treated as a given — an individual's identity must be collected and recorded in association with services rendered or purchases made. But must this always be the case? Are there no situations where transactions may be conducted anonymously, yet securely? We believe that there are and will outline a number of methods and technologies by which anonymous yet authentic transactions may be conducted.

Joint International Report: The Netherlands and Ontario, Canada

The Dutch Data Protection Authority (the "Registratiekamer" or RGK) and the Information and Privacy Commissioner for the Province of Ontario, Canada (IPC) are both privacy protection agencies that oversee compliance with their respective jurisdiction's privacy laws. The RGK and IPC decided to pool their resources and collaborate in the production of a report exploring privacy technologies that permit transactions to be conducted anonymously. The first international paper of its type includes a survey of companies that might be expected to offer such technologies, and organizations that might use them. In addition to anonymous transactions, the range of security features commercially available for use and the types of services actually being used by various organizations were also examined (see 2.1, Methodology). The RGK and IPC felt that a joint report outlining the practices followed in their respective jurisdictions would shed some light on this little-studied but extremely important area where the future of privacy-protection in an electronic world may lie.

Theoretical Basis for the Joint Report

Prior to this joint report with the IPC, the Registratiekamer, within its legally vested scope of powers and duties, conducted a study on the possibilities offered by conventional information systems and communications technologies for curbing the use of identifying data, particularly within information systems. This study, conducted in collaboration with the TNO Physics and Electronics Laboratory of the Netherlands Institute for Applied Scientific Research (TNO–FEL), formed the theoretical basis for the international study. The results of the Registratiekamer/TNO–FEL study are detailed in the companion volume to this report (Volume II).

Background

Consumer polls have repeatedly shown that individuals value their privacy and are concerned with its potential loss when so much of their personal information is routinely stored in computer databases, over which they have no control. Protecting one's identity goes hand in hand with preserving one's ability to remain anonymous — a key component of privacy. While advances in information and communications technology have fuelled the ability of organizations to keep massive amounts of personal data, this has increasingly jeopardized the privacy of those whose information is being collected. Minimizing identifying data would restore privacy considerably, but would still permit the collection of needed information.

When assessing the need for identifiable data during the course of a transaction, the key question one must start with is: how much personal information/data is truly required for the proper functioning of the information system involving this transaction? This question must be asked at the outset — prior to the design and development of any new system. But this is not the case today. This question is rarely asked at all since there is such a clear preference in favour of collecting identifiable data, "the more the better." However, with the growth of networked communications and the ability to link large numbers of diverse databases electronically, individuals will become more and more reluctant to leave behind a trail of identifiable data. What is needed is a paradigm shift away from a "more is better" mindset to a minimalist one. Is it possible to minimize the amount of identifiable data presently collected and stored in information systems, but still meet the needs of those collecting the information? We believe that it is.

The technology needed to achieve this goal exists today. We will describe some of the privacy technologies that permit one to engage in transactions without revealing one's identity by introducing the concept of an "identity protector." The notion of "pseudonymity" will also be introduced as an integral part of protecting one's identity. These technologies are available now and are within our reach; what is needed is the will to implement privacy technologies over the tracking technologies that are in use today.

When organizations are asked what measures they have in place to protect privacy, they usually point to their efforts at keeping information secure. While the use of security measures to prevent unauthorized access to personal data is a very important component of privacy, it does not equal privacy protection. The latter is a much broader concept which starts with the questioning of the initial collection of the information to ensure there is a good reason for doing so and that its uses will be restricted to legitimate ones that the data subject has been advised of. Once the data have been collected, security and confidentiality become paramount. Effective security and confidentiality will depend on the implementation of measures to create a secure environment.

Alternatively, instead of restricting the focus to security alone, a more comprehensive approach would be to seek out ways in which technology may be used to enhance the protection of informational privacy or data protection. We use the term "privacy

technologies" to refer to a variety of technologies that safeguard personal privacy by minimizing or eliminating the collection of identifiable data.

Not only are measures that safeguard privacy becoming an important mark of quality, but increasingly, consumers are demanding that organizations pay attention to their privacy concerns. Social acceptance of demands for one's personal information, without adequate assurances of protection, appears to be on the decline. Not only do consumers wish to maintain control over their personal data and be informed of its uses, but insufficient protection will be reason enough for consumers to take their business elsewhere — to companies that follow privacy-protective practices.

Privacy Laws and Codes of Conduct

Respect for individuals' privacy, particularly with respect to the computer processing of personal data concerning one's self, is a fundamental principle underlying data protection. In Europe, data protection principles may be found in several instruments such as the Council of Europe's Convention 108 (Treaty for the protection of persons with regard to automated processing of personal data, Council of Europe, January 1981 (1988 Official Journal of Treaties, 7). One of the objectives of these principles is to ensure that personal privacy is safeguarded when new information technology applications are developed. The principles are reflected in various European laws and regulations such as the Dutch Data Protection Act (WPR) and the draft EU-directive SYN 287. In addition, the OECD's Guidelines on the Protection of Privacy and Transborder Flows of Personal Data (September 1980) is internationally acclaimed as a "code of fair information practices" with respect to the treatment of personal information.

One of the basic principles in both the OECD guidelines and Convention 108 is the principle of "purpose specification." The quantity and nature of personal data that an organization is permitted to collect is limited by the purpose of the collection. The primary rule is that the data be relevant and sufficient, but not excessive for the stated purpose. In other words, the personal information to be collected must be needed to carry out the stated purpose.

This principle also seeks to ensure that restraint is exercised when personal data are collected. In accordance with this principle, one may question when identifying data is being sought from individuals where it is not necessary to do so. This is associated with the "use limitation principle," where the purpose specified to the data subject at the time of the collection restricts the use of the information collected. Thus, the information collected may only be used for the specified purpose (unless consent has been obtained for additional uses).

Another important data protection principle is "transparency" or "openness." People have the right to know what data about them have been collected, who has access to that data, and what the data are being used for. The principle of transparency simply means that people must be made aware of the conditions under which their information is being kept and used.

The principle of transparency may also be used to explain the logic behind the data processing underlying a collection — asking for identifying information in a situation that does not strictly require it, must be questioned. Indeed, the collection and use of personal data for identification purposes when not truly necessary (where alternatives are available), cannot be supported in relation to the principles noted above. Since these data protection principles are incorporated into most privacy laws such as the Ontario *Freedom of Information and Protection of Privacy Act (FIPPA)* and the Dutch Privacy Act (Wet persoonsregistraties), or EU-directive SYN 287, in some situations, the unnecessary collection of identifiable data may have a direct bearing on compliance with these statutes.

Information Systems

An information system is broadly defined as a system which provides organizations with the information required to conduct various activities. There are generally three types of information systems: transaction-processing systems, programmed decision-making systems, and decision-support systems. Transaction-processing systems collect and keep track of information relating to a transaction. Examples range from direct marketing systems, mail order catalogue purchasing systems, telephone records systems, and so forth.

Programmed decision-making systems process data in accordance with formal, structured procedures. The system is programmed, on its own, to complete the entire order from the time it is received through its entire processing, without any human intervention. Examples include hotel reservation systems, payroll accounting systems, money transaction systems for automatic teller machines, flight reservations systems, etc.

Decision-support systems assist in the decision-making process by using the information collected to either generate potential solutions or additional information to assist in the decision-making process. Examples include systems for calculating mortgages, management information systems, recommended itinerary systems, etc.

The one common feature of all these systems is that their use entails the collection and processing of personal information. Whenever an individual (the user) comes into contact with an information system, the service provider usually requires that they identify themselves through some means.

The Structure of an Information System

The elements of an information system consist of the following: user representation (containing a means of identification), service provider representation, and a database(s) containing the data required for the information system to function. The database usually consists of two files, the privileges file and the audit file. The privileges file contains the user's privileges (which the service provider would check to see whether he/she was eligible for the various services offered). The audit file records the use of the information system and can charge the user of a service or track what services were used by whom, at what times. Using the example of a health club, the privileges file would contain a record of the user's entitlements, i.e., that a particular user was entitled to use certain

services such as the use of the tennis facilities (five times a month), the squash courts (four times a month), but not the golf course (which the user had not paid the required additional fee). The audit file would keep track of the actual uses of the various privileges and charge the user a per-use fee for any additional services that the user was not entitled to (i.e., playing golf).

A user representation can take the form of an account number, a membership card or a smart card. A service provider representation represents the interests of the organization and controls access to the organization's various resources (through passwords; tiered levels of authorization to increasingly sensitive information, etc.).

The Processes in an Information System

The use of an information system entails the following processes: authorization; identification and authentication; access control; auditing and accounting. We refer to a process as an exchange of information between two or more elements within the information system. In conventional systems, the user's identity is usually viewed as being essential to the performance of all the above processes. For example, one's identity is used within the authorization process to identify and record instances involving a user's privileges. Once the user's identity has been collected, it will travel throughout the various processes involved in the information system. We will suggest that this need not be the case. One must examine whether the user's identity is truly required for the operation of each of these processes.

We will propose that a user's identity is only necessary during the processes of authorization and accounting. For the processes of identification and authentication, access control, and audit, a user's identity may be sheltered through some type of "identity protector." We will describe how technologies of privacy may be used to separate one's true identity from the details of one's transactions through the use of "pseudo-identities."

The Identity Protector

An identity protector may be viewed as an element of the system that controls the release of an individual's true identity to various processes within the information system. Its effect is to cordon off certain areas of the system which do not require access to true identity. The identity protector works in such a way as to protect the interests of the user. One of its most important functions is to convert a user's actual identity into a pseudo-identity — an alternate (digital) identity that the user may adopt when using the system.

Alternate identities also exist in conventional systems such as bank account numbers, social insurance/social security numbers, health insurance numbers, etc. But these cannot be viewed as pseudo-identities since they may easily be linked to one's true identity. In the privacy-protective systems of the future, the identity protector would most likely take the form of a smart card controlled by the user, which could generate pseudo-identities as desired.

An identity protector performs the following functions:

- generates pseudo-identities as needed;
- converts pseudo-identities into actual identities (as desired);
- combats fraud and misuse of the system.

Since the identity protector is under the control of the user, he/she can set it to perform a variety of functions such as revealing one's actual identity to certain service providers but not to others. When an identity protector is integrated into an information system, the user may use the services or engage in transactions anonymously, thereby elevating privacy to an all-time high.

When an identity protector is introduced into an information system, two domains are created: an identity domain and a pseudo domain — one in which the user's actual identity is known and accessible, and one in which it is not. The identity protector functions so as to separate the two domains and may be applied anywhere in the system where personal data can be accessed. A simple guideline for designers of new information systems is to minimize the identity domain wherever possible and maximize the pseudo domain.

The identity protector permits the designer of a system to minimize the personal data stored in a database. In effect, the service provider would not record the user's privileges or activities under their true identity but rather, under their pseudo-identity. While the service provider must be able to determine what the user is authorized to do, this may be accomplished without learning the user's true identity. Since the identity protector acts somewhat as an intermediary between the user and the service provider, it must be trusted by both parties. However, there is no disadvantage to service providers since their ability to verify the user's privileges/eligibility for services remains intact. Indeed, the identity protector is designed in a way which prevents fraud and improper use. The latter can take various forms ranging from prevention, detection, and correction. It can prevent the user from using his/her anonymity as a shield to commit fraud, and, in appropriate circumstances, can lead to having the true identity of the user being revealed to the service provider and/or the authorities. For example, cryptographic techniques may be used to prevent a sum of money (digital cash) from being used anonymously more than once, or a service being used but not charged to the user.

Implementation Techniques

Thus far we have discussed a theoretical approach using the concept of an identity protector in the design of systems that would permit individuals to interact anonymously with service providers. Below, we will outline several specific techniques for introducing an identity protector into an information system. Specifically, encryption techniques involving digital signatures, blind signatures, digital pseudonyms and trusted third parties, will be described. Additional readings are provided in the companion text (Volume II) for those wishing to explore these techniques in greater detail.

Digital Signatures

A digital signature is the electronic equivalent of a handwritten signature. Just as a signature or sealing wax on a document is proof of its authenticity, a digital signature provides the same, if not better, authentication. It provides the necessary assurance that only the individual who created the signature could have done so, and it permits all others to verify its authenticity. A particular type of encryption, "public key encryption," considered to be the most reliable and secure form of encryption ever developed, forms the basis for digital signatures.

In a public key system, two keys are created for each individual — one private, one public. The private key is known only to the individual while the public key is made widely available. When an individual encrypts a document with his or her private key, this is the equivalent of signing it by hand since the private key is unique to that individual alone. Any third party may decrypt the message using the individual's public key, which corresponds only to his/her private key. If the document is successfully decrypted, then one has the necessary assurance that it could only have been created by that individual. Otherwise, one would not have been able to decode it. Digital signatures thus provide proof of a document's authenticity — that the document originated from the sender. For a more detailed description of this cryptographic technique, please refer to Volume II.

Blind Signatures

The blind signature, created by David Chaum of Digicash, is an extension of the digital signature, but with one critical feature added: it ensures the anonymity of the sender. While digital signatures are intended to be identifiable and to serve as proof that a particular individual signed a particular document, blind signatures provide the same authentication but do so in a non-identifiable manner. The recipient will be assured of the fact that the transmission is authentic and reliable, but will not know who sent it. One application involving blind signatures is the use of "digital cash" which may be used as an electronic form of payment that can be transmitted over computer networks. Just as cash is anonymous, digital cash is anonymous in that it cannot be traced to a particular individual — it is considered to be "unconditionally untraceable." However, the service provider is assured of its authenticity; all that is missing is the ability to link the transaction to a particular person. In describing his system of blind signatures, Chaum adds that it also provides much-needed protections against fraud and abuse of the system. For a detailed description of blind signatures, we refer you to Volume II.

Digital Pseudonyms

A digital pseudonym is a method of identifying an individual through an alternate digital pseudo-identity, created for a particular purpose. It permits users to preserve their anonymity by concealing their true identities. While users are not "known" to service providers in the conventional sense, they are, nonetheless, known by their pseudonyms, for the purposes of conducting transactions.

Digital pseudonyms build upon the blind signature technique. However, in this instance, it is the service provider who assigns privileges to a given pseudonym (user) by creating a blind signature. The user keeps the allotted privileges (for example, five uses of the tennis courts per month), and uses them as desired. Again, we refer you to Volume II for a more detailed discussion of this subject.

Trusted Third Parties

A trusted third party is the term used for an independent third party who is trusted by both the user and service provider alike (comparable to a "digital attorney"). This party can be entrusted with keeping such things as the master key linking digital pseudonyms with the true identities of their users. The trusted party knows that the relationship between a user's true identity and pseudo-identity must be kept completely secret. However, if certain conditions require it, the trusted party will be permitted to reveal the user's identity (under previously agreed upon terms) to a service provider. The conditions under which an individual's identity would be revealed must be known to both the user and service provider prior to entering into an agreement with the trusted party.

Moving from Conventional Technologies to Privacy Technologies

The most important prerequisite to moving in the direction of privacy technologies is to start by asking whether identifiable information is truly needed when a new information system is being contemplated, or an existing one upgraded. If the client, the systems designer and supplier ask this question right from the start, privacy is sure to be addressed. The creation of some form of identity protector within the system must also be a crucial part of the design phase. To recap, the identity protector is a term for all those functions within an information system that protect the user's true identity, such as the creation of pseudo-identities. A pseudo-identity is a pseudonym that the user may assume for the purpose of engaging in a particular transaction or service. The guiding principle should always be to keep the identity domain as small as possible, thereby maintaining the absolute minimum amount of identifiable information. The actual implementation of an identity protector may be done in a number of ways, usually involving advanced encryption techniques (best left to systems designers and technical staff).

The point to emphasize is that it is indeed possible to collect less identifiable data, or unlink the data from an individual's true identity through the use of pseudo-identities. It is only the application of privacy technologies that is lacking, not the technologies themselves.

IPC–RGK Joint Survey

The primary purpose of the joint survey was to assess the types of privacy technologies commercially available for keeping anonymous the identity of individuals during the rendering of services. We also wanted to establish an estimate of the companies offering such technologies, as well as assessing the types of technologies available for protecting the security and confidentiality of information transmitted electronically.

These technologies could be offered through a variety of means such as hardware, software, network communications, encryption products or application systems design practices. Our only criteria was that they not be at a theoretical stage, in other words, they had progressed beyond the lab test phase; we wished to survey applications and products that were already built and being offered in the marketplace.

Another element of the survey involved the potential users of these products, in an effort to determine the extent to which these technologies were actually being used and the degree of awareness or interest in their availability.

The specific objectives of the survey were:

- to establish an estimate of the number of information technology (IT) providers that were making privacy technologies available to their customers;
- to determine whether organizations falling under the jurisdictions of the RGK and IPC were using or considering privacy technologies to keep the identity of individuals anonymous during service delivery.

Methodology

The sample consisted of 100 IT providers; 50 companies from the Netherlands and 50 from Ontario, Canada. The following types of IT providers were sampled: product vendors; service providers (application and systems software developers, consulting firms, online service providers, security associations). A small sample of technology users was also included; these consisted of organizations falling under the respective jurisdictions of the RGK and IPC.

The IT providers and user organizations selected were contacted by telephone and asked to participate in a short survey. A copy of the questionnaire may be found in Appendix A. Detailed product brochures and technical specifications were also requested.

Findings

Tables 1 to 3 present the responses obtained from the IT providers sampled.

TABLE 1 *Privacy Technologies to keep Identity Anonymous*

Information Technology:	Yes		No	
	IPC %	RGK %	IPC %	RGK %
Available now	10.0	33.3	90.0	66.7
May be available in the future	8.0	28.6	92.0	71.4
Asked to develop	6.0	33.3	94.0	66.7

Table 1 presents the percentage of IT providers presently offering or developing privacy technologies that permit an individual's identity to be kept anonymous during service delivery. In Ontario, only 10% of the providers sampled offered products capable of

keeping identities anonymous. This contrasts with a much larger number of Dutch companies, 33.3%, who presently offer anonymous technologies. In Ontario, only four providers contacted had any thoughts of developing such technologies in future. We should add, however, that the types of anonymous technologies referred to here are not the kind that use encrypted techniques such as digital pseudonyms.

In the Netherlands, however, one company, Digicash, is known for its work in developing anonymous technologies based on public key encryption and blind signatures. In Ontario, the main technology involved in maintaining anonymity was the prepaid or stored-value smart card — a card that is "loaded up" with cash and used anonymously. Such cards ensure anonymity because, like cash, they carry no personal identifiers. Another way in which anonymity was preserved was through the use of a "remailer" service wherein an individual's true identity was stripped from the data prior to being forwarded electronically to a third party. In the Netherlands, privacy technology tends to be more application driven as in the anonymous recording and processing of data in tax files, personal information systems, and payroll processing systems.

While the incidence of companies offering anonymous technologies was low, most respondents, when asked why they were not devoting more time and effort to such product development, said there was presently no demand for it from their customers. If there was, they would reconsider. Therefore, if customers' awareness of such technologies and their benefits (more privacy and anonymity) increased, so would the likelihood that suppliers would develop products offering these features.

Table 2 presents the percentage of IT providers who had developed or were considering developing products that protected the security of information transmitted electronically.

TABLE 2 *Availability of Products that Protect the Security of Information*

Information Technology:	Yes		No	
	IPC %	RGK %	IPC %	RGK %
Available now	56.0	81.0	44.0	19.0
May be available in the future	12.0	66.7	88.0	33.3
Asked to develop	32.0	76.2	68.0	23.8

Over half (56%) of the Ontario IT providers sampled had developed products that protected information security. Twelve per cent of the providers sampled were considering developing such products in the near future. A much higher percentage of the Dutch providers sampled — 81%, presently offer such technologies. Thus, the majority of companies contacted offered products or applications that protected the security of information transmitted electronically.

Security examples involving financial transactions such as interactive banking were identified as being in special need of stringent security measures. Large multinationals, banks and other financial institutions were regarded as being the driving force behind

security-enhancing technologies. This was due to increases predicted in the electronic transmission of sensitive financial transactions and the use of electronic currency. It was said that the highest degree of confidence needed to be associated with the authenticity and integrity of financial transactions, requiring the development of "fail-safe" information systems, to boost consumer trust and confidence.

There was a substantial difference in the responses of the Ontario and Netherlands IT providers regarding the offering of such products in the future. Two-thirds of the Netherlands companies sampled expected to be developing encryption products for information security in the near future. In Ontario, however, only 12% expected to be doing so. This difference could in part relate to how often these companies had been approached to develop such products. The companies in the Netherlands had more than twice as often been asked to develop such products than their counterparts in Ontario. This may have to do with a major public debate that took place in the Netherlands in 1994, regarding the use of encryption techniques, triggered by proposed legislation for the use of encryption in telecommunications services.

When asked specifically what types of technologies they used to protect security, cryptographic techniques such as encryption, both public key and symmetric systems, were named most frequently (DES; RSA; DES in conjunction with RSA or IDEA). Several references were also made to the use of PGP (pretty good privacy). The use of digital cash was also noted several times as a way to preserve anonymity during electronic transactions requiring electronic forms of payment.

In addition, each of the following was named at least once as a means of protecting information security: unique one-time transaction numbering systems, frequently changing encryption keys, and the use of smart cards for PIN code protection.

Not only was the need for security perceived to be critical during electronic transmissions, one respondent pointed to the growing need for secure transmissions during mobile (wireless) telephony. Since wireless communications are no longer restricted to telephones, extending well beyond to wireless data transmissions and networked communications, there will be a strong demand for the development of secure wireless networks (one example being the Mobitex Network which makes use of data encryption techniques).

Unlike privacy technologies designed to preserve anonymity, products relating to the protection of information security were far more widely available. Several Dutch companies felt that politically, the demand for information security would increase, perhaps making legislation in this area a necessity. Information highway applications such as e-mail and electronic service delivery were especially viewed as being in need of stringent security controls.

One reason for the low degree of awareness of anonymous technologies, contrasted against the high awareness of technologies protecting information security, is the fact that technology has commonly been associated with keeping information secure.

Protecting privacy, however, in the form of keeping an individual's identity anonymous, is a relatively new concept — one that has rarely been considered by vendors and suppliers, or requested by customers. The much-needed awareness of the existence of such technologies among users is virtually non-existent at the present time.

Table 3 presents the types of technologies used in the products offered by IT providers.

TABLE 3 *Types of Information Technologies Offered*

Information Technology:	To Preserve Anonymity		To Protect Information Security	
	IPC %	RGK %	IPC %	RGK %
Encryption	—	12.5	100.0	90.0
Smart Cards	60.0	25.0	—	—
Application Design	20.0	50.0	—	10.0
Anonymous Remailing	20.0	12.5	—	—
Total	100.0	100.0	100.0	100.0

In Ontario, smart cards, or specifically prepaid "stored-value cards" appear to be the most popular method of preserving anonymity, while encryption was the key technology (100%) used to protect information security. In the Netherlands, the use of encryption was also comparably high (90%) for security purposes. But the use of smart cards in the Netherlands (25%), was lower than in Canada (60%). The RGK expects to see similar developments in the Netherlands in the near future. A greater use of applications design (50%) was made in the Netherlands to preserve anonymity. By "application design" we mean the privacy protective design features of applications developed in the creation of new information systems.

All providers in the area of systems development indicated that they could easily design features into any system to keep an individual's identity anonymous (through such techniques as encryption and smart cards), if their clients asked for these features. Again, however, what is lacking is the demand for such features, which in turn is related to the lack of awareness of their benefits among users.

IT Users

Due to an extremely low response rate from the organizations contacted (government, trade and industry), no quantitative reporting of users' responses will be presented. Instead, a narrative description of respondents' views will be presented below. It should be noted that only one of the government organizations contacted in Ontario was making any effort to protect anonymity: an internal procedure had been developed that allowed the identities of staff to be kept anonymous while communicating with the organization's human resources department. Of the companies contacted in the Netherlands, one bank was using a software application to produce internal reports

where data about clients was kept anonymous; another bank used pseudo-identities (numbers) instead of the true names of individuals; and another company separated the flow of personal from other data — maintaining a link between the two through a numerical system.

Respondents' Views

Most respondents (providers and users alike) felt that there was increasing pressure on both the public and private sectors to provide additional security for electronic transmissions of information, especially in the areas of electronic commerce and electronic payment systems. While overall awareness in this area appears to be growing, the same cannot be said for technologies that preserve anonymity. Since these technologies are relatively new and difficult to grasp conceptually, this should come as no surprise. In addition, one could speculate that most organizations would not wish to have anonymity maintained — quite the contrary, they would like to collect more, not less, identifiable information (that would permit the development of personal profiles and the tracking of purchasing patterns and activities). The public must be made aware of the availability and benefits of privacy-enhancing technologies so that they will be better positioned to make informed choices.

General Observations

- There was a general lack of understanding as to the difference between privacy and confidentiality; survey respondents tended to use the two words interchangeably. While confidentiality (keeping information secure and inaccessible to unauthorized parties) is an important component of privacy, it is just that — one component. The areas covered by privacy are much broader, extending from limitations on the initial collection of personal data (whether it is truly needed), to restrictions on its use to the purpose specified, to prohibitions on any secondary uses (without the express consent of the data subject).

- When asked what products/technologies were offered to protect privacy, most IT providers identified security-related products that served to keep personal data confidential (secure from third party interception). The importance of maintaining security and confidentiality were clearly understood. But this was not the case for the importance of maintaining privacy through anonymity. While the great majority of IT providers expected to see dramatic growth in the area of security-related technologies (firewalls, encryption products, etc.), they had no similar expectations for the growth of privacy-enhancing technologies.

- It was clear that IT providers would respond to market forces: if the demand is there, they will build it. Even a minimal growth in awareness of privacy technologies and acceptance of anonymous services could yield a demand significant enough to warrant the attention of IT providers. Public awareness and education are key.

- Information technology will be one of the primary ways to ensure the protection of privacy in electronic transactions and networked communications.

Discussion of Findings

When embarking upon this joint project, the Registratiekamer and IPC wished to outline a variety of technologies that protected privacy by preserving an individual's anonymity during service delivery. Another wish was to provide some empirical evidence of what was generally believed to be true — that privacy technologies known to be in existence were not widely known or used by providers or the public. Thus, the findings outlined in this report came as no surprise since this proved to be the case. Awareness of these technologies tended to be somewhat higher in the Netherlands, but not as high as one might hope in light of the public discussions about encryption which had taken place, and the presence of a prominent company (Digicash) that specializes in the development of such technologies.

While one may be disheartened by the overwhelming lack of awareness (particularly in Ontario), one may also view this as a great opportunity — awareness can increase dramatically if the word gets out. The challenge that must be faced is how to "get the word out there," and get it out to enough people to make a difference. Due to the present lack of demand for such technologies from the public, there is little reason for IT providers to develop them. The need for public education cannot be over-emphasized: this is one area which is unlikely to be discovered (or understood) without some assistance. Nor can we expect service providers or organizations to encourage the development of such awareness — the task will fall upon privacy commissioners and privacy advocates. We hope that efforts such as this joint report will contribute to increasing awareness, and to begin going down the road to greater understanding.

Conclusions and Recommendations

In this report, it has been submitted that an individual's identity is only truly necessary for certain parts of an information system, namely, during the processes of authorization and accounting. We have introduced the concept of an "identity protector" and described how technologies of privacy involving encryption and digital pseudonyms may be used to separate one's true identity from the details of one's transactions and communications. Such practices would lead to far fewer collections of identifiable information and would thus greatly enhance the protection of privacy.

Among the challenges that lie ahead will be the reluctance of both public and private sector organizations that wish to collect more, not less, identifiable information (until the benefits of collecting less are understood and organizations come to realize that identifiable information is not always necessary for their activities). Add to this a public which generally lacks awareness of the benefits to be had through the use of anonymous technologies (never having been exposed to them), and the challenge grows even larger. To help meet these challenges, we make the following recommendations.

Recommendations

1 International information systems design standards should be developed incorporating the need to examine whether an individual's identity is truly required for the operation of various processes within the system. Attention should be explicitly directed to the introduction of an identity protector, which functions to separate the identity domain from the remaining pseudo-domains.

2 At the design stage of any new information system, or when revising an existing one, the collection and retention of identifiable personal information should be kept to an absolute minimum. Only that which is truly needed should be collected and maintained in an identifiable form (as opposed to a pseudonymous form).

3 Consistent with the privacy principle that information systems should be transparent and open to view to data subjects, they should also provide users with the ability to control the disclosure of their personal information. Data subjects must be placed in a position to decide for themselves whether or not their identity should be revealed or maintained in an information system.

4 Data Protection Commissioners, Privacy Commissioners and their staff should make every effort to educate the public and raise levels of awareness in the area of privacy-enhancing technologies. The use of privacy technologies by public and private sector organizations should be also encouraged. The message that it is now possible to preserve an individual's anonymity during service delivery should be included in all public outreach efforts. The benefits to be derived to individuals from the use of anonymous technologies are far-reaching and will ensure the continuation of privacy protection in a fully networked world.

5 Data Protection and Privacy Commissioners should ask the parties involved to review the use of identifiable data in light of privacy protection principles and make use of privacy-enhancing technologies wherever possible. The unnecessary collection of identifiable data, where appropriate, should give rise to further action to promote compliance with existing statutes.

DESIGN: nectar design + communications www.nectardesign.ca

CONTACT INFORMATION:

General inquiries should be directed to:
Tel: (416) 326-3333
1-800-387-0073
Fax: (416) 325-9195
TTY (Teletypewriter): (416) 325-7539
e-mail: info@ipc.on.ca
Website: www.ipc.on.ca

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

Ann Cavoukian, Ph.D.

INFORMATION AND PRIVACY COMMISSIONER OF ONTARIO