Office of the
Privacy Commissioner
of Canada

Commissariat à la
protection de la vie privée
du Canada

# Identity, Privacy and the Need of Others to Know Who You Are: A Discussion Paper on Identity Issues

**September 2007**

# Table of Contents

## Target Audience

This discussion paper is intended primarily for the lay reader.  For this reason, the paper avoids technical language where this does not sacrifice accuracy.

# Introduction

What is "identity," and how is it relevant to privacy? That is the central focus of this paper. How we identify ourselves to individuals, businesses and government organizations (in other words, how we "manage" our identity) has profound implications for our relationships. Identity plays a central role in the tug-of-war between efforts to protect privacy and efforts that push us towards a "surveillance society." For example:

- The Government of Canada has in recent years raised the possibility of introducing a national identity (ID) card. In a 2003 survey, 30 per cent of Canadian respondents strongly agreed that everyone should have a government issued ID card that they must carry at all times, and 23 per cent somewhat agreed.[1] But would Canadians still be so accepting of a national identity card if they had the opportunity to become more fully informed of its privacy implications and limitations in enhancing security and preventing crime? Depending on its design, a national identity card could give government departments and other organizations great surveillance powers over individuals without significantly increasing government efficiency or public safety. Underpinning a national identity card system would almost certainly be a database of those participating, or "enrolled," in the system. This enrolment database would contain personal information about the entire population. In addition, the use of a single national ID card number would make it simple for organizations to amass comprehensive profiles about individuals, possibly in real time – an anathema to a democracy that purports to respect privacy.

[1] In 2003 the Surveillance Project, a multi-disciplinary research group affiliated with the Department of Sociology at Queen's University, received funding from the Social Sciences and Humanities Research Council of Canada to study the globalization of personal data (GPD). A key component of the GPD project was an international survey involving 9,000 individuals in eight countries (Brazil, Canada, China, France, Hungary, Mexico, Spain and the U.S.). These findings were taken from that survey.

Identity is not just an issue in the relationship between individuals and governments. Many businesses want to identify their customers so they can personalize their services, track their customers' behaviour, and target their marketing based on that behaviour. In addition, "list brokers" – companies that compile and sell personal information to other companies and government agencies – want identifying information to help in developing the "profiles" of individuals, profiles that they then sell to businesses or governments. The ways in which individuals identify themselves can either facilitate or limit profiling.

Requiring individuals to identify themselves at every turn can rob them of the right to participate in society without having their every movement and interaction monitored and linked to them. This deprives them of an important aspect of privacy, the ability to go about their daily activities anonymously. Equally, intelligently managed "identity systems" can preserve, and even strengthen, privacy and many other important rights that flow from respect for privacy.

Indeed, there are many good uses of identity. The federal program, "Government On-Line," is meant to stimulate the provision of better, faster, trusted and more convenient and accessible government services over the Internet. Providing such services may require that individuals have a way of identifying themselves to government in the on-line environment. E-commerce – Internet banking and sales over the Internet, for example – also require secure forms of identification. The move away from paper-based to electronic health records, where records held in different locations can be connected to improve patient care, also requires finding appropriate means of linking the health record to the appropriate individual.

Appropriate means of identifying individuals can help protect them against someone else "stealing" their identity and personating them in business relations – getting a loan, for example. Properly managed, identity can even protect

individuals in personal relationships – such as by preventing someone from assuming the online identity of an estranged spouse in order to cause havoc in the spouse's personal life by sending out emails or other communications purporting to come from the spouse. Individuals also need government-issued documents that attest to their identity (a passport to facilitate international travel, for example), their authorization to do something (such as drive a car) or their entitlement to receive benefits (government-sponsored health care). Finally, identity can play a role in protecting our security.

How can we protect privacy in a world where identity is central to our lives? It is not a case of identity or privacy. How can we manage identity in a way that fulfills the legitimate goals of government and business, while respecting the needs – and rights – of individuals to have their privacy respected?

Despite Canada being a world leader on identity issues, legislative and policy measures have not been able to stay abreast of the progress of identity technologies and their implications for privacy. Compounding this problem is the lack of understanding of identity issues among Canadians – for example, about the benefits and drawbacks of a national identity card system. "Identity" is not well understood outside a small group of experts.

Identity issues can indeed be complex. A 2002 report[2] by the National Academy of Sciences of the United States highlights many of the challenges that arise when introducing identity systems:

- What is the purpose of the system?
- What is the scope of the population that would be issued an ID and, presumably, be recorded in the system?

[2] Stephen Kent and Lynette Millett, eds., National Academy of Sciences, Computer Science and Telecommunications Board, *IDs – Not That Easy: Questions About Nationwide Identity Systems* (Washington, DC: National Academy Press) 2002. Available at: http://www.nap.edu/catalog/10346.html (accessed February 1, 2007).

- How would the identities of these individuals be authenticated (proved)?
- What is the scope of the data that would be gathered about individuals participating in the system?
- Who would be the user(s) of the system (as opposed to those who would participate in the system by having an ID)? What entities within the government or private sector would be allowed to use the system? Who could contribute, view, and/or edit data in the system? (In essence, this asks who are the insiders of the system, and what powers they have.)
- What types of use would be allowed? Who would be able to ask for an ID, and under what circumstances?
- Would participation in and/or identification by the system be voluntary or mandatory?
- Would participants have to be aware of or consent to having their IDs checked (as opposed to, for example, allowing surreptitious identification checks through technologies such as facial recognition)?
- What legal structures protect the system's integrity, as well as the data subject's privacy and due process rights, and determine governments' and relying parties' liability for system misuse or failure?

Beyond these policy questions are a complex series of technical, security and economic issues relating to identity.

Canadians need the opportunity to understand the role that identity plays in society and the privacy issues related to identity. This discussion paper is intended to do just that – help inform Canadians about the role of identity in shaping their privacy rights. This paper cannot examine every aspect of identity. Entire books, some of them highly technical, have been written on the subject. This paper instead seeks to describe core concepts relating to identity as simply as possible, but with sufficient detail for individuals to understand the privacy

implications of identity and to be able to contribute to public policy debates about identity issues.

The paper examines the following aspects of identity:

- The meaning of “identity” and the various components of identity – for example, “authentication,” “attributes,” “identifiers,” “identity management,” “identity systems,” and “tokens;”
- Who is interested in identity, and why? For example, when is it appropriate to have some means of “identifying” individuals, and what role should identity play in matters of national security?
- Conflicts and common interests in identity management;
- Privacy issues associated with identity; and
- Proposals for rethinking identity to address privacy issues.

# Identity Basics

## *What is "Identity"?*

What do we mean when we speak of our "identity" and "identifying" ourselves to others? Perhaps the easiest way to understand identity in reading this paper is to think of it as "how a person is known" by another person or organization. For example, our family members know us in certain ways (including birth name, personal traits and education), and so do our employers and the many service providers we encounter. They all have a notion of who we are – that is, of our identity. In other words, an identity can be thought of as a set of information about an individual that distinguishes that individual from others *in a particular context.*

More precisely, an identity is a set of "attribute" information (or "claims") about an individual. Attribute information can be anything:

- An individual as he or she is known to another individual (name, physical appearance, membership in a social group);
- An individual as he or she is known to an employer (full name, employee number); and
- An individual as he or she is known to government (name, Social Insurance Number (SIN) or health card number).

In each case, at least one of the attributes of the person is in fact *unique* in the context, in the sense that *no* other person in that context is supposed to have that attribute. The person's family name is unique to the family members (unless they are named after another family member), the employee number and, possibly, the full name are unique to the employer, and the SIN or health insurance number is unique to the federal government.

"**Identifier**:" An attribute that is unique in a given context is called an "identifier."[3] What makes it an identifier is that only one person (presumably) is associated with that particular identifier.

Attributes that are unique in one context and that are therefore identifiers may not serve as identifiers in another context because they are not unique in that other context. A person's first name – Harold, for example – is an attribute that may be an identifier for direct family members because it is unique in that context. In the street, "Harold" may no longer be an identifier, since there are many people named Harold. "Harold" is still an attribute of the person, but it is not an identifier because it is not unique to one person. A person's full name may be unique (and therefore an identifier) in a city or possibly even beyond that, but it is not likely to be unique in a country. That is why society has created identifiers that are designed to be unique even in larger society. In Canada, the Social Insurance Number is supposed to unique among all Canadian residents. Health card numbers are supposed to be unique among the residents of a province. A particular health card number can be linked to one specific individual.

Today, people typically use (or are identified on the basis of) different identifiers in different contexts, rather than using a unique identifier for all of their activities. We are selective in disclosing our identifiers. In other words, we identify ourselves to our government through our SIN, but we don't use our SIN to identify ourselves to our friends. Instead, we use our name. We may use our

[3] "An identifier is a piece of information that names or indicates a person, a process, an application, a location (such as a place on earth or a CPU memory address), a tangible object (such as a book, a text file, or a device), or any other type of entity or grouping of entities. User identifiers are identifiers that represent users (i.e., individuals or groups of individuals) in their interactions with relying parties. ... Within a designated context, user identifiers enable relying parties to distinguish between the individuals they interact with; this is known as identification." See: Stefan Brands, "Secure User Identification Without Privacy Erosion," (2006) 3:1 University of Ottawa Law & Technology Journal 205-223, http://www.uoltj.ca/articles/vol3.1/2006.3.1.uoltj.Brands.205-223.pdf.

loyalty card number to identify ourselves to a retail store, and our frequent flyer number to identify ourselves to an air carrier.

**Identification**: Identifiers enable others to distinguish between the individuals they encounter. This is known as identification. Identification is the process of someone (or some business or government) trying to determine a person's identifier, so that it can "look up" all the associated attribute information for that party. Consider this non-electronic example: When you meet a friend on the street, the friend recognizes your appearance, thereby "identifying" you. The friend can "retrieve," from memory, other information associated with you. The friend is using your identifier to retrieve other "attribute" information about you – your membership in the same club or school group, for example. When talking with that same person on the phone, your unique voice "signature" may serve as an identifier, particularly when you combine it with mentioning your name. When corresponding with your friend, your e-mail address may suffice to enable your friend to "identify" you. When you give a government institution your SIN, you have identified yourself to the institution. It can then retrieve other "attribute" information about you that it holds in its files.

Knowing the identity of someone is not always important. In many cases, identifiers serve only as a means for others to get information about our attributes ("attribute" information) that is of interest to them. For example, a bar owner may use a driver's licence to ensure that a patron is of legal age to enter the bar. The fact that a person is of legal age is the attribute of interest to the bar owner. A police officer may use the same licence to ensure that a person is entitled to drive. The entitlement to drive is also an "attribute." In both cases, it is not truly necessary to know the identity of the person. The bar owner or police officer merely want to confirm that the individual has certain attributes – age or majority or authority to drive. Ways to provide attribute information without disclosing identity – thus protecting privacy – are discussed more fully below.

Dr. Stefan Brands presents a list of many identification methods:[4]

- Birth names, corporate names, nicknames, and author pseudonyms;
- E-mail addresses, telephone numbers, postal box numbers, and URLs [Universal Resource Locators];
- Fingerprints, iris or retina scans, and DNA samples;
- User account identifiers with ISPs [Internet Service Providers], banks, utility companies, and so on;
- Credit cards, debit cards, calling cards, and loyalty tokens;
- Employee badges, sports club membership cards, and hotel key cards;
- Social security numbers, health insurance numbers, passports, and driver licences;
- Online usernames (*e.g.*, for instant messaging and chat rooms), cookies, and SSL [Secure Sockets Layer] certificates; and
- MAC [Media Access Control] addresses, IP [Internet Protocol] addresses, smartcard serial numbers, Bluetooth identifiers, GSM [Global System for Mobile Communications] IMEI [International Mobile Equipment Identity] numbers, RFID [Radio Frequency Identification ] tag identifiers, and other addresses of networked user devices.

All of these specific unique identifiers can be used in particular contexts to distinguish one individual from another – in other words, to "identify" the individual.

**Identity management**: The concept of "identity management" is central to the discussions in this paper. The general definition of identity management is in essence "anything that has to do with the management of identities throughout their life cycle." However, identity management does not always involve

[4] Stefan Brands, "Secure User Identification Without Privacy Erosion," (2006) 3:1 University of Ottawa Law & Technology Journal 205-223, http://www.uoltj.ca/articles/vol3.1/2006.3.1.uoltj.Brands.205-223.pdf.

identifying an individual. Identity management could merely involve passing around attribute data (such as a card that attests that the holder is of legal age to enter a bar), without any accompanying identifiers. To the extent identifiers must be included, these can be "local" identifiers that reduce the likelihood of linking information about a person and tracing the person's activities.

## *Identity Systems*

Many discussions about improving security flowed from the attacks of September 11, 2001, in the United States, and later attacks in Spain and the United Kingdom. Those discussions focused in part on better means of singling out individuals who pose a threat to security, and some governments have proposed a national ID "card" as an essential element of better security. (Elsewhere in this paper, particularly in Appendix A, we discuss the weaknesses of claims that a national security card would enhance national security). However, a national ID card is merely one component of a complex identity "system" that must be built around the card. To quote the U.S. National Academy of Sciences:

> "System" . . . implies the linking together of many social, legal, and technological components in complex and interdependent ways. The success or failure of such a system is dependent not just on the individual components, but on the ways they work—or do not work—together. Each individual component could, in isolation, function flawlessly yet the total system fail to meet its objectives. The control of these interdependencies, and the mitigation of security vulnerabilities and their unintended consequences, would determine the effectiveness of the system.
>
> A nationwide identity system would also consist of more than simply a database, communications networks, card readers, and hundreds of millions of physical ID cards. The system would need to encompass policies and procedures and to take into account security and privacy considerations and issues of scalability, along with human factors and manageability considerations (if the requirements of use prove too onerous or put up too many barriers to meeting the goal of the relying party, that party might try to bypass the system). The system might need to specify the participants who will be enrolled, the users (individuals, organizations, governments) that would have access to the data, the permitted uses of the data, and the legal and operational policies and

> procedures within which the system would operate. In addition, a process would need to be in place to register individuals, manipulate (enter, store, update, search and return) identity information about them, issue credentials (if needed), and verify search requests, among other things.[5]

It is important to keep in mind the complexity of society-wide identity systems. They are not by any means a "quick fix" to security problems.

## *Offering Evidence to Establish Confidence in a Claim about One's Identity —"Authentication"*

When individuals identify themselves, they are stating who they are. However, this does not *prove* that they are who they say they are. In other words, simply presenting an identifier does not prove that the identifier belongs to them. Anyone can walk into a bank to apply for a mortgage and state they are Mr. Smith, but that does not prove they *are* Mr. Smith. The process of offering evidence to establish confidence in one's claim about identity is called "authentication." To "authenticate" (establish confidence in) their claim about their identity ("I am John Smith"), individuals can rely on a range of evidence. These items of evidence are called "authenticators." For example, a birth certificate can be used to help authenticate identity, as can a passport or dental record.[6]

In ancient times, societies did not generally need sophisticated evidence to authenticate identity. Everyone in a community knew everyone else. They were

[5] Stephen Kent and Lynette Millett, eds., National Academy of Sciences, Computer Science and Telecommunications Board, *IDs – Not That Easy: Questions About Nationwide Identity Systems* (Washington, DC: National Academy Press) 2002 at 13-14. Available at: http://www.nap.edu/catalog/10346.html (accessed February 1, 2007).

[6] "In communication and transaction settings, authentication is typically understood as the process of confirming a claimed identity. This involves two steps: first a user must present a user identifier (such as "John Doe" or "Employee 13579") that uniquely represents the user in the verifier's context. The second step, identity authentication, involves verifying that the presenter of the user identifier is authorized to do so – in other words that the presenter is the user to whom the user identifier has been assigned." See: *Encyclopedia of Privacy* [Two Volumes], William G. Staples (ed.), ISBN: 0-313-33477-3, Greenwood Press.

able to identify others by recognizing attributes such as voice, physiological traits and other biometric clues such as hair or eye colour. However, as societies grew and became more complex, individuals had to find ways to establish their identity to complete strangers, businesses and governments which could not recognize them by attributes such as voice or psychological traits. Over time, various means evolved to do this, including "token-based" mechanisms (such as birth certificates and passports) and reference checks (where a trusted person known to the organization that has asked for evidence of identity is asked to vouch for the identity of a new person).

### *Authenticating Authorization or Entitlement*

In many cases, the authentication that an organization or agency needs is evidence of an individual's authorization or entitlement, not evidence of their actual identity. Organizations or agencies may want to be confident, for example, that the person before them is authorized to enter a building, or is entitled to receive benefits. Identity is not the real issue.

In fact, in most of society's transactions, organizations are not interested in evidence to establish the identity of the person, but are instead interested in evidence to show something else. For example:

- A merchant is interested in establishing that the customer is entitled to use the credit card presented to the merchant;
- A bus driver is interested in knowing that the ticket (or "token") used to enter the bus is valid. The driver has no interest in knowing anything about the passenger, unless the passenger is using a ticket such as a student discount ticket, in which case the driver may want some proof of student status to confirm the passenger's right to use a student ticket. Even here, the bus driver does not need to know the identity of the person, merely that the person possesses the attribute of being a student;

- A government transportation authority could issue a driver's licence indicating that the person holding the card is entitled to drive a car, and provide a means (perhaps by using biometrics) to assure a police officer that the card belongs to that driver. This is called "attribute authentication."[7] The officer could verify that the person is authorized (or "entitled") to drive, without knowing the person's name, age or address. Being able to identify the driver by name is irrelevant (and in fact always was irrelevant to the question of the authority to drive). Information about the identity of the driver could be made available to the police officer if there is a legitimate public interest in the officer having access to the information, such as to assist in a criminal investigation. However, the release of identifying information beyond the authorization to drive should be the subject of public debate and should not simply occur by default, as it does now, because of the structure of today's driver's licences.

Where a business or government agency doesn't really need to know the individual's identity, but merely that the individual is authorized to do something (use a credit card) or entitled to receive something (a government benefit), individuals can protect their privacy by restricting the identifying information that they surrender about themselves. This limits the ability of others to monitor their activities and profile them.

## *Means to Establish Confidence in a Claim about Identity, Authorization or Entitlement*

Individuals can authenticate their identity or attributes (such as authorization or entitlement) by offering evidence of any or a combination of the following:

[7] Attribute authentication is the process of establishing an understood level of confidence that an attribute applies to a specific individual: Stephen T. Kent and Lynette I. Millett, *Editors*, Committee on Authentication Technologies and Their Privacy Implications, National Research Council, *Who Goes There? Authentication Through the Lens of Privacy* (Washington, D.C., The National Academies Press, 2003).

- something they are (for example, their DNA, the pattern of their iris, or facial features);
- something they have (for example, a bus ticket ("token"), driver's licence, credit card, or passport); and
- something they know (for example, a password or personal identification number (PIN)).

Combinations of these items of evidence can be used to reduce the risk that someone is identified or authorized incorrectly. In a nuclear facility, for instance, it may be necessary to show a building access card (something you have) and have a machine read the individual's iris (something you are) so that the reading can be matched with an image of the individual's iris that is stored on the card or in a separate database. This combination of "single-factor" methods is called multi-factor authentication. The one "factor" is the building access card and the other is the characteristics of the iris.

If the nuclear facility required only a weak single-factor authentication,[8] such as a pass code, it might be possible to enter the facility easily by stealing the pass code. However, a strong one-factor authentication method may be much stronger than weak multi-factor authentication. In other situations, such as establishing that a person is old enough to enter a bar, the harm caused by relying on a weak authentication would be less serious.

More generally, authenticators differ in the degree of confidence they can provide about a person's identity or authorization to do something. A passport is

[8] "Single-factor identity authentication ascertains that the presenter possesses something associated with the presented user identifier that is not generally accessible. This can be something the user knows (such as a password or a cryptographic key), something the user has (such as a chip card), or something the user is (i.e., a user biometric). ... To strengthen the process of identity authentication, several single-factor methods may be combined, resulting in multi-factor authentication." See: *Encyclopedia of Privacy* [Two Volumes], William G. Staples (ed.), ISBN: 0-313-33477-3, Greenwood Press.

generally (depending on the trustworthiness of its issuer) better evidence of identity than a sports club membership card. This is because an applicant for a passport will have provided several authenticators that, when combined, offer strong evidence of identity. A person applying for a passport must provide the following items of evidence to help to establish identity:

- an official document that attests to birth in Canada or Canadian citizenship (for example, a birth certificate from a Canadian province or a certificate of Canadian citizenship);
- at least one other document, such as a driver's licence, health care card, other provincial identification card, certificate of Indian Status or Old Age Security card;
- two identical photos, one signed by a guarantor attesting that the photo is a true likeness of the passport applicant;
- a statement by a guarantor who has known the applicant for at least two years and who certifies the identifying information supplied by the applicant.

A very clever criminal might still be able to obtain a passport fraudulently despite the relatively stringent evidence required to obtain the passport. A person must provide evidence of Canadian citizenship (a birth certificate, for example) and one other piece of identification, such as a driver's licence. But these documents can be (and too often have been) forged. To have confidence in the process of establishing identity, one must have confidence in the integrity of these documents, called "root" documents or "breeder" documents, as authenticators. In essence, the passport application process relies on potentially imperfect proof of identity, since it is possible to obtain fraudulent driver's licences and birth certificates. However, requiring several of these potentially imperfect documents (and the guarantor's certification) increases the difficulty for someone to obtain a passport fraudulently, since he or she would need to require a multiplicity of false authenticators – documents and certifications – not just one or two.

An applicant for a membership in a sports club, on the other hand, will likely need to provide only very weak authenticators – perhaps a name and address. (Some argue that stating one's name is not an authenticator at all, merely the presentation of a claim about one's identity).

If offered a choice, a business that needs to be confident in the claim by an individual about their identity or attributes would be better advised to rely on the passport instead of the membership card. However, customers would likely rebel at the privacy intrusions that being required to show a passport would entail, since this would provide the business with information about potentially sensitive information such as country of birth and nationality. The passport number also provides an identifier that can help link together other information about the individual, posing a threat to privacy.

Requiring too little evidence to prove identity, authorization or entitlement might make the organization or person relying on that proof vulnerable to fraud or some other harm. In a rational world, the degree of proof required about one's identity or authorization to do something would vary with the importance attached to "getting it right." For example, the operator of a nuclear facility will want a great deal of certainty that the person seeking to enter the facility is one of the authorized employees, while the bus company would suffer only a minor loss if it trusted someone's claim about being entitled to a student discount.

## *The Limits of Authenticating Identity for Enhancing Security*

Much is sometimes made about the need for individuals to carry identifying documents to enhance national security or control crime. This is one of the arguments used in many countries in supporting a national identity card. *However, proving identity says little about the trustworthiness of an individual.* Offering evidence to prove identity merely shows that the individual is who he

says he is; it indicates nothing about whether the person is a criminal or a terrorist.

Only if the authenticating information is used, for example, to check whether the person's name appears in a database of criminal records, can authentication be part of the process of establishing a person's trustworthiness. However, this will not identify those who have committed crimes but have not yet been caught or identified by police, nor can it identify those who intend to commit crimes. And requiring an airline passenger to show a passport or driver's licence says nothing about whether the passenger is carrying an explosive device. To determine that, it is necessary to search the person.

There is a privacy-protective solution. Technology allows people to present "credentials" directly that show whether or not they have a criminal record, for example, without revealing more than that as a first step.

## Protecting Privacy by Using Unlinkable Identifiers

Identification processes can make it much easier to compile comprehensive dossiers on individuals**.** In some situations, the individual has no choice in deciding what to offer as proof in identity matters. To obtain a passport, an individual must disclose place, country and date of birth. To obtain a driver's licence, an individual must give date of birth and address. To obtain a bank loan, individuals must disclose information such as name, Social Insurance Number and perhaps place of work and salary.

Other times, however, individuals can choose which of their identifiers to disclose. For example, a person may create[9] their own distinctive username as an identifier for an online discussion group.

[9] Some describe the process of creating a distinctive identifier for a given context as "self generating" an identifier.

In short, beyond the identifiers that individuals are required to disclose for specific purposes, they can be selective about the identifiers they disclose to others. They may identify themselves by one name when they use the Internet, and by another name when they join a book club. Individuals may choose to disclose certain identifiers in one situation, and other identifiers in another.

Limiting the number of and varying the identifiers that individuals disclose makes it more difficult for others to link information about them that may be held by different organizations. For example, a bank may have an individual's account number, but not their passport number. A Canada Border Services Agency (CBSA) inspector may have the individual's passport number, but not the bank account number. The only way to link the data contained in their separate files would be if they both had access to bank account numbers and passport numbers. There is no "common identifier" that allows information contained about an individual in one file to be linked with information held in another file.

Both the bank and the CBSA could try to use the individual's name as the basis for correlating their respective information holdings on the individual, but relying on the name alone when combining files ("data matching") carries a great risk of error. Matching data contained in two separate files about a person with a common name ("John Smith") carries the risk that the two files may not relate to the same person. The information in the combined file would then be unreliable and, likely, useless.

On the other hand, if both the bank and the CBSA collected the individual's Social Insurance Number, having this "common identifier" in both databases would make it very simple to combine the information contained in them. In this way, common identifiers can pose a great threat to privacy. (Legislation or government policies may limit the combining of databases in this way, but here we are merely discussing the technical issues surrounding common identifiers.)

Some readers may question the need to keep separate personal information held by different organizations and government departments (some describe this as keeping personal information in different "silos"). However, files are kept separate for an important reason – to prevent governments and the private sector from compiling comprehensive files about individuals. Such files are the mark of authoritarian regimes, and they have largely been absent – at least until recently – from democratic societies. Comprehensive files also violate one of the key elements of the right to privacy in a democratic society – the right of individuals to control what information others can acquire about them.

## *Privacy via Using "Bearer Tokens"*

Individuals can get even greater privacy protection through a system of "bearer tokens." For example, a government agency could issue a card ("token") authorizing the holder to receive provincial health care benefits. Tokens can be designed to prevent someone other than the legitimate holder from using them. And they can also be designed so that if the individual uses a token to obtain health services, no record connecting that specific individual to the service would be created. In other words, the individual could remain anonymous to the health care system, so it would not be possible to monitor the individual and build a profile of his or her use of the system. Of course, in many situations it could benefit the individual to be identified to the health care system, since the system could then be used to retrieve other information about the individual that could be useful when treating the individual. But the individual would decide whether to participate in a system that would allow such information to be retrieved and linked to the person.

As discussed above, a driver's licence could also be structured as a "token" that would prove the authority to drive, but offer the person examining the token no information beyond that, and would not permit the driver to be tracked. Only if

there was a legitimate need for the police to have additional information or track the individual, would information beyond that showing the driver's entitlement to drive be released to the police.

There may be legitimate reasons for wanting to be able to link individuals with the services provided to them, and governments or businesses may be able to show a justification for tracking an individual's interactions with them. However, most situations do not require that honest individuals disclose their real names as a first step. For example, in the example of the driver license, a driver could be asked to "disclose" his real name only in case of suspicion. For this, another proof of identity could be used.

## Conclusion

To this point, this paper has explained some of the basic aspects of identity systems. It has showed that how we manage our identities can have major implications for privacy. The next section of this paper examines what we need to do to manage our identities in such a way as to protect privacy, while responding to the legitimate needs of government, business and individuals for information about identity, authorization or entitlement.

# Who is Interested in Identity?

Governments, the commercial sector and individuals all have important, and sometimes conflicting, interests in the policies, technologies and laws built around identity. Here we discuss some of the interests that are driving the sometimes distinct approaches of these groups to identity issues.

### Governments

Governments have a duty to provide many services to citizens and to protect them from harm. That means providing services such as medical care and other benefits programs, and protecting individuals from violence and other criminal activity such as fraud and theft.

Today's national security concerns revolve to a great extent around fears of terrorist attacks. Governments are exploring new identification systems – for example, the system built around a national identity card – to improve security.

In addition, governments may need to become involved in identity matters to respond to the demands of other governments. Canadians travelling abroad are generally required to present a passport containing specific information about the passport holder, such as name, and date and country of birth. Canada has no choice but to accept these demands if it wants to facilitate international travel by Canadians. That means that Canada must develop identity processes – in this case, the passport application – that attest to the identity of the passport holder in a way that satisfies foreign governments.

Governments are also responsible for providing documents that confirm entitlement to services such as health care, or that confirm the authorization to carry out an activity (driver's licences, for example).

Clearly, governments must be involved in several aspects of identity management. But their role is not merely to seek better means to identify their citizens in the name of national security or the efficient administration of government programs. A good example is voting. This involves being able to distinguish between individuals to ensure that nobody can vote more than once, but privacy (in fact, anonymity) is also a requirement. Governments must also espouse and protect the elemental rights of a democracy, including privacy. This can create a conflict between the desires of governments to obtain better assurances about the identity of those with whom it deals (or wants to control) and the obligations of governments to respect privacy.

**Businesses**

Many businesses want to know that the individual with whom they are dealing is in fact that individual, not an impostor. For example, a bank does not want to give a mortgage loan to a person who has "stolen" someone else's identity and is pretending to be that person. Businesses also want to ensure that the means individuals use to pay are legitimate. In other words, they want to ensure that a person who uses a credit or debit card is authorized to use that card. Finally, many businesses want to learn about individual consumers (consumer preferences, lifestyle and income, for example) to improve marketing efforts to those consumers.

**Individuals**

Above all, individuals have a privacy interest in controlling what others can learn about them. This has important implications for identity management, since individuals will often want identity management policies that preserve their privacy and their anonymity.

Individuals want to ensure that any identity management system relating to them doesn't unreasonably or unnecessarily require them to disclose personal information that can then be used to profile them. In short, most want the least amount of intrusion into their lives that is necessary for the proper functioning of society and their own role in it. Hence, in relations with commercial organizations, many individuals do not want identity systems (credit cards or loyalty cards, for example) to enable commercial organizations to profile them or target them for marketing.

In some cases, individuals want to avoid a commercial or government organization receiving any identifying information about them. This is why some people pay cash when they shop. In other words, they want the freedom to choose what identifiers they present to others, and the availability of options to allow them to have that freedom, including, in some cases, options that allow them to remain anonymous.

Individuals also want to avoid the social exclusion that can flow from refusing to use some forms of identification – for example, a national identity card, or even a credit card – since choosing not to use such cards may arouse suspicion and/or lead to a denial of services or other discriminatory treatment.

Individuals also have an interest in protecting themselves against someone stealing their identity. Identity theft in essence involves someone using another person's identifier in a particular context to "masquerade" as them, which may allow a criminal access to certain services. For example, an identity thief may attempt to do any of the following:

- Make purchases using credit cards, or obtain loans;
- Deal with government (for example, to secure benefits or to obtain a passport);

- Take harmful actions in the name of the individual – such as where a vindictive ex-spouse might try to send malicious emails in the individual's name.

Identity thieves may also commit other criminal offences and then use the innocent owner's identity when caught and convicted. The innocent owner may face the sometimes near-impossible task of showing that he or she was not the person who committed the offence.

Identity theft is not just a theoretical problem. The first few weeks of 2007 saw commercial organizations lose the personal information of hundreds of thousands of Canadians, making those Canadians vulnerable to identity theft. As well, fraudsters will sometimes call a financial institution pretending to be another individual (a ruse called "pretexting") in order to deceive the institution into releasing personal information, which can then help the fraudster steal that person's identity.

As we move into an electronic society, the risks of being a victim of identity theft increase through ruses such as "phishing" (an online version of pretexting, explained in greater detail below).

To reduce the risk of identity theft, individuals require security measures. The degree of security provided by these measures varies. A credit card provides some security in that the legitimate owner's signature is set out on the back of the card. When an individual signs a credit slip, the sales clerk compares the signature on the card with the signature on the strip. A Social Insurance Number alone is an identifier without any protection, since anyone can use the number. A card containing the Social Insurance Number provides a degree of authenticity, but there is still no obvious way of ensuring that the person holding the card and using the number is in fact its legitimate owner. A card provided by a trusted source and containing a photograph of the owner would provide greater security.

As well, in order to participate in many functions of society, individuals need governments to provide them with trusted documents that attest to their identity, such as passports and birth certificates. Society has also decided that credentials are important for the proper functioning of society – for example, trusted documents that prove entitlement (e.g., to health benefits) or authorization (e.g., to drive). At the same time, individuals want to avoid the inappropriate government surveillance that can flow from some identity systems.

Just as businesses and governments want to verify the identity of individuals, individuals want to be able to verify the identity of the organizations and government agencies they encounter. This is commonly referred to as "mutual authentication." Indeed, proper authentication of the parties with whom individuals interact can help reduce the risk of pretexting and phishing.

## *Conflicting and Common Interests in Identity Management*

Because the interests of the three groups – individuals, businesses and governments – in identity management may differ, conflicts may arise over the best identity management policies.

### Conflicting Interests

For individuals, the main source of conflict comes from the loss of privacy some identity systems entail, and the lack of offsetting benefits. There are two points of contention. First, how much privacy is given up when engaging in a new identity system, and second, is that the absolute minimum necessary to achieve those benefits? In some cases, the benefit may be so marginal that even the least intrusive identity system would not be justified. People may want the benefits that can arise from identity systems, for them individually and for society, but they may also want these systems to be as unintrusive as possible.

Individuals may in particular fear that some identity systems – national identity cards or Social Insurance Numbers (SIN), for example – will lead to massive data matching and profiling both by governments and the private sector, which will then be able to compile information about an individual held in separate databases by using the identity card number or SIN as the "common identifier."

Before the advent of computing technology, locating and combining personal information held in separate filing systems ("data matching") was highly labour-intensive. This provided a significant degree of privacy protection to individuals whose personal information was kept in separate record keeping systems. This was so even if a common identifier – for example, a Social Insurance Number – was used as the index for storing information about the individual in each of the systems. That protection has all but disappeared with digital records, which can instantly be electronically pulled from different databases if a common identifier is used to index entries in the databases.

Individuals may also balk at the extent of proof of identity – the number of identifiers and pieces of evidence of proof of identity – that they are required to present in some dealings with government or business.

On the other hand, government and businesses, unless their curiosity is limited by law, policy or technology, typically react initially by requiring more identifying information about individuals than they strictly need, even when there are no clear or justifiable purposes for acquiring that information.

**Common Interests**

The interests of individuals and businesses in identity management do not always conflict. Both groups want to avoid fraudulent transactions. For example, to avoid credit card fraud, both groups may therefore support similar measures –

a PIN (personal identification number) on a credit card, for example, or an online identity verification scheme. However, even if they both agree on the need for security, they may differ in their concept of the means to achieve that security.

Individuals and governments can also find common ground in identity management. Neither group, in theory, wants those who are not entitled to government benefits to have access to those benefits. In theory, governments, like individuals, want to avoid practices that violate the rights of individuals. Both groups want to see governments provide secure, trusted documents that attest to the status of the individual where justifiably required – as a Canadian citizen, a driver or an individual who has a right to state-sponsored health care.

Businesses and governments may both be interested in the greater surveillance capabilities offered by some forms of identity management – common identifiers, for example – since these help to link and combine personal information held in separate files. Identity management may also help a business trace those who engage in fraud against the business.

Individuals, businesses and governments all have an interest in preventing "phishing." Phishing may occur, for example, when someone fraudulently sends an individual an email appearing to be from the individual's bank. The email asks the individual to visit a web site disguised to look like that of the legitimate bank. At this fraudulent site, the individual may be asked for passwords and account numbers. If the individual falls for this ruse and provides the information, the fraudster then has the necessary information to get access to the individual's account.

Because of security threats such as phishing, individuals want to be assured that they are dealing with their own bank, not a fraudster masquerading as their bank.

Individuals who download updates to their computer anti-virus programs want to be assured that the source of the download is legitimate, so that they don't unwittingly download software from a fraudulent web site that will damage their computer files or rifle through those files to identify passwords and account numbers. Individuals who receive correspondence from a government agency want to be assured that the correspondence does not come from a fraudster. In short, individuals have legitimate needs to require authentication by the organizations that they deal with before they provide their own identity credentials.

Even where individuals, businesses and government have common interests in identity management, there are differences in degree. Governments might be tempted to impose greater security measures, through identity requirements such as identity cards, than their citizens will tolerate.

# Rethinking Identity Management to Better Protect Privacy

## *A Clean Slate for Examining Identity Systems*

We could examine identity management from either of two perspectives:

- We could start with the assumption that the current means we use to prove identity, authorization or entitlement are acceptable from a privacy standpoint. This would mean, in essence, that we would be accepting those identification processes because "we have always done it this way." We would examine (perhaps through what could be called an "identity system impact assessment") only proposals for new means to manage our identities – a national identity card system, for example, or a new border-crossing card system; or
- We could start with a clean slate and look at all situations where identity might be at issue, including situations where we already establish our identity or authorization in a particular way, such as by producing a driver's licence that discloses name, address and age. We would not assume that, because we have used a certain identity management method in the past, it is appropriate to continue using that method (especially in light of "scaling up" and "upgrading" paper-based processes to electronic processes). The appropriate method for showing identity, authorization or entitlement might turn out to be very different than those now used. Choosing the "clean slate" approach would mean assessing the privacy impact of all identity methods, current and proposed.

The "clean slate" option requires rethinking identity management processes that are already in use, but it enables us to develop schemes that are consistent from a privacy and policy perspective. It also allows us to revisit past identity schemes

and measure them against underlying privacy and other public policy goals, such as limiting the amount of personal information that individuals should need to disclose to go about their normal, lawful activities. Do such schemes respect privacy to the greatest extent possible while serving other legitimate interests, such as the interest of governments in providing security for its citizens, the interests of businesses in preventing fraud, and the interests of individuals in avoiding being the victim of fraud or theft related to the misuse of their identities?

Starting from a clean slate will also prevent government agencies and businesses from attempting to continue using, or to expand, existing identification schemes (such as requiring a Social Insurance Number) that may lead to serious privacy intrusions in some situations.

## *Setting the Privacy Parameters for Identity Management*

A democracy that purports to value individual autonomy and privacy must place limits on when and how a person is required to identify him- or herself and, how much information is required to participate in society. At the same time, identity policy must address the legitimate needs of governments and the private sector for information about an individual that enables them to conduct business with the individual, provide services to or administer programs for the individual.

Some readers might question the need to rethink the ways now used to prove identity, authorization or entitlement. However, our society possesses increasingly advanced tools that allow the type of extensive surveillance that is characteristic of authoritarian societies. We may have the good fortune to live under governments that in general respect rights, but no Canadian, and no citizen of any democratic country, should take it for granted that their governments will always reject authoritarian methods. That is why we should pay such careful attention to limiting the types of surveillance available to

governments, including the surveillance that current and potential identity systems can facilitate.

Similarly, Canadians should consider the privacy implications of identity in their relationships with the private sector. Limiting the types of surveillance available to governments may also mean limiting the capabilities of the private sector to conduct surveillance through identity management, since information obtained by the private sector through surveillance can easily and lawfully[10] find its way into the hands of a curious government. Thus, the collection of personal information by the private sector can bolster government surveillance.

**Right to anonymity as the starting point**: Many people would probably agree that if they are simply walking down a street, they shouldn't be required to identify themselves to a police officer or other agent of the state unless there is a justifiable purpose. They would also probably agree that they should be able to use cash so that they can remain anonymous when they buy groceries or board a bus. Many would likely agree that, *unless there is a valid reason for requiring individuals to identify themselves, the right to anonymity should be the norm.* The right to anonymity is the highest right individuals should have, and it should be overruled only for justifiable reasons. Even when the right to anonymity is overruled for justifiable reasons, only the minimum amount of personal information needed for the task at hand should have to be disclosed or shared. The individual could of course choose to share identifying information with others, but that would be the individual's choice, not the requirement of government or business or the inevitable by-product of technologies or identity systems that facilitate acquiring information about the individual.

[10] See, for example, section 7(1) of the *Personal Information Protection and Electronic Documents Act* (known as *PIPEDA*), S.C. 2000, c. 5. This section allows organizations, in certain circumstances, to collect personal information and disclose it to government without the consent of the individual to whom it relates.

**Anonymity through "tokens":** If anonymity is to be, or remain, the "default" state for individuals, then authentication via tokens (or "bearer tokens") is a critical means to preserve that anonymity. The bus ticket is a low-technology token. Technologists have developed more sophisticated electronic "tokens" that also enable individuals bearing those tokens to remain anonymous.

What could this mean in practice? It could mean that individuals could conduct business anonymously, so that they would leave no trail of information about themselves. The low-tech version of this is paying for goods with cash. The high-tech version is paying for goods with a prepaid electronic cash card that leaves no information to connect the purchase with the individual. In both cases, the purchaser remains anonymous. Contrast this with purchases by credit card, where the merchant will see the name on the card, and the credit card company will keep a record of all purchases – allowing the tracking and profiling of the individual.

Similarly, the showing of a driver's licence as proof of age when entering a bar could play into the development of a web of surveillance around the person who simply wants to prove age of majority – surveillance that is completely unwarranted for the vast majority of people going about their lawful daily activities. The anonymity-enabling alternative is for a trusted organization, such as a government agency, to issue a card (a "token") with the young person's photograph attesting that an individual has reached the age of majority. That may not please the bar owner, who may want to know as much about customers as possible for marketing purposes, but it will protect the privacy of the customer by allowing the customer to choose how much about him- or herself that the bar owner (and related businesses) can learn.

In the nuclear facility example, a facility access card could contain a biometric, such as a fingerprint. The person holding the card would place his or her finger on a reading device, which would compare this fingerprint to that in the card. If

they match, the person's authorization to enter the facility is established. No other information about the individual need be presented to the guard at the facility (although additional information would have been presented at the time the card was created and the trustworthiness of the person would also have been verified before the card was issued).

**Make Authentication Requirements Proportionate to the Circumstances:** In settings where governments or businesses are justified to reject anonymity, individuals may need to authenticate themselves.

Proportionality is key. Limits are needed on the type and extent of authentication required. The degree of certainty about a person's identity or attributes required should be the minimum necessary to achieve the legitimate objectives of the identification or authorization process. A student seeking to buy a reduced-price student bus ticket should not be required to provide a Social Insurance Number, a biometric and a driver's licence in addition to a student card. However, the level of certainty required for an employee in a nuclear facility must be greater, since the consequences of mistakenly allowing someone into the facility may be serious. For example, obtaining a prospective employee's name will enable the employer to do a criminal records check. Obtaining information about the employee's educational background will enable the employer to verify that the applicant has the necessary qualifications to work in the nuclear industry.

Note that a strong authentication method does not necessarily reveal more information about an individual than a weaker authentication method. It is possible to have strong authentication and yet reveal very little personal information.

**Selective disclosure of identifiers**: Anonymity protects privacy, but anonymity may not always be feasible, or desirable. In situations where anonymity is not appropriate, the next best thing is for individuals to be able to use different

identifiers for different types of transactions or interactions with others. These identifiers must be structured so that they cannot be linked with each other ("unlinkable identifiers"). This makes it difficult to correlate information relating to these transactions and interactions filed in different databases according to those unlinkable identifiers. Indeed, this is how much of the world has functioned traditionally.

If different organizations use distinct identifiers, the organizations cannot easily correlate the information that each holds about an individual. It may still be possible, of course, to make correlations with "attribute" data such as name and address, but the use of separate identifiers can greatly reduce the possibility that information in different databases can be linked. Since not all organizations care about the privacy of the individuals whose data they hold, it may be necessary to enact measures that discourage the collection of identifiers (common identifiers) that permit the linking of personal information held in separate databases. It is also important to remember that many organizations may believe that they protect privacy, but they are really speaking about "security" against outsiders, not about misuse of personal information – such as through linking databases – by insiders.

**Using Strong Authentication to Protect against Identity Theft:** Individuals have a strong interest in obtaining documents that attest to their identity or authorization to do something such as drive or purchase goods, but that cannot be easily misused by others. It might seem that organizations would also want to prevent such misuse as well. However, the interests of organizations and individuals do not always coincide. In some cases, the organization (a bank, for example) might tolerate a deficient identification or authorization scheme – that used for the cards used to withdraw cash from bank machines, for example. It might tolerate these deficiencies if the losses they permit are not significant or if the organization can pass the losses on to customers through higher credit card interest or banking fees. Governments may therefore need to step in to compel

organizations to adopt identification and authorization schemes that are less vulnerable to identity theft.

## *The Way Forward with Identity*

### The Roles of Parliament and the Federal Government

**Safeguarding privacy rights**: Under international law and the *Canadian Charter of Rights and Freedoms*, Parliament has a duty to safeguard the privacy and autonomy rights of individuals. Parliament and federal government departments and agencies should therefore not introduce identity measures that unnecessarily diminish the right of privacy if other, less intrusive measures, will achieve the same objective.

Parliament should review Canada's existing data protection legislation – the federal *Privacy Act* and the *Personal Information Protection and Electronic Documents Act* (*PIPEDA*) – to ensure that these laws do not contain deficiencies that serve as easy routes for government and the private sector to conduct unwarranted surveillance by exploiting current or emerging identity systems. The focus of legislative measures should also be on avoiding identity systems that have unnecessary surveillance capabilities, even if those capabilities are not being used at present. The mere existence of those surveillance capabilities may represent an irresistible attraction for future governments.

**The *Privacy Act***: The federal *Privacy Act* regulates the collection, use and disclosure of personal information by federal government institutions. However, the Office of the Privacy Commissioner has often criticized the ineffectiveness of the *Privacy Act* in protecting the privacy rights of Canadians in their interactions with the federal government.

In the context of identity management, the Act lacks any provision dealing with common identifiers and linking personal information held in distinct databases

(data matching). Common identifiers such as Social Insurance Numbers or identity card numbers can be used for data matching. Yet the *Privacy Act* imposes no significant controls on the collection, use or disclosure of common identifiers. The Act allows a government institution to collect personal information if it relates directly to an operating program or activity of the institution.[11] There is no requirement in the Act that the collection of the information be in any way necessary or reasonable. Furthermore, the Act allows government institutions to disclose personal information to various other bodies in a wide range of circumstances, even without the consent of the individual.[12]

The lack of control over data matching has been a long standing criticism of the *Privacy Act*. As the Privacy Commissioner's 2004-05 *Annual Report to Parliament on the Privacy Act* noted:

> Although government use of data matching (or "computer-matching") arguably poses the greatest threat to individuals' privacy, the *Privacy Act* is silent on the practice. Privacy Commissioners (bolstered by Parliamentary Committees) have all recognized the dangers inherent in excessive and unrelated data collection. All have recommended amending the *Privacy Act* to ensure that government institutions link personal records in discrete systems only when demonstrably necessary, and under the continued vigilant oversight of the Privacy Commissioner of Canada. The recommendations have not been followed through.

The same report noted that the federal Treasury Board had issued guidelines in 1989 outlining the steps departments should take before matching data, including submitting a detailed proposal for the Privacy Commissioner's review. However, the Office of the Privacy Commissioner reported that it had received few notices, despite the likely frequency of the practice.

[11] Section 4.
[12] Section 8(2).

The *Privacy Act* applies to federal government institutions. Amending the Act to add rules on data matching can help to limit the combining of personal information held in disparate databases. Then, even if government institutions use a "common identifier" such as the Social Insurance Number or a national identity card number to index files concerning individuals, they might be prohibited (at least, unless and until a future government relaxes the law) from combining the data contained in those files.

Some also criticize the lack of enforcement powers in the *Privacy Act.* Even if a government institution violates the Act's already weak provisions, the Privacy Commissioner of Canada has no direct powers of enforcement. The Privacy Commissioner can investigate the alleged violation and report her findings publicly and to Parliament, but functions as an ombudsman in so doing.

The core elements of the *Privacy Act* have remained almost unchanged since the Act came into force in 1983. Despite numerous recommendations to update the legislation, no government in the past quarter century has moved to make the Act more effective in protecting the privacy rights of Canadians. Given the likely interest of government in the surveillance possibilities that some identity systems (national identity card systems, for example) would permit, it seems unlikely that the federal government will be interested in amending the Act to limit the surveillance possibilities that such identity systems provide. Pressure by public interest groups and privacy bodies may be the only forces that will lead to greater protection.

As we move into an electronic society, more than mere *Privacy Act* amendments may also be needed to prevent unnecessary/unjustifiable powers in identity systems, by both outsiders and insiders. This is particularly so in an era when we have moved from non-electronic to electronic identity systems. The privacy risks increase dramatically in this electronic environment.

***Personal Information Protection and Electronic Documents Act* (*PIPEDA*)**: *PIPEDA* fares somewhat better as a tool for protecting the privacy of individuals in identity matters. The Act applies to organizations engaged in commercial activities, including those that for other purposes (for example, employment) are regulated by the provinces. *PIPEDA* therefore covers the retail sector, publishing and insurance companies, the service industry, manufacturers and other organizations, such as those in the health sector.

Section 3 of the Act identifies the purpose of its data protection provisions:

> The purpose of this Part is to establish, in an era in which technology increasingly facilitates the circulation and exchange of information, rules to govern the collection, use and disclosure of personal information in a manner that recognizes the right of privacy of individuals with respect to their personal information and the need of organizations to collect, use or disclose personal information for purposes that a reasonable person would consider appropriate in the circumstances.[13]

Unlike the *Privacy Act*, *PIPEDA* contains an explicit recognition of the need to balance the privacy rights of individuals with the needs of organizations for personal information, and also imposes a requirement that the purposes for which the organization collects, uses or discloses personal information be reasonable. The Principles set out as a schedule to the Act also state that organizations must not collect personal information indiscriminately, and that they must collect information by fair and lawful means.[14]

In addition, personal information must 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.[15] This limits the use or disclosure of personal information for data matching purposes. Unless an organization obtains the

[13] Section 3.
[14] Principle 4.4.
[15] Principle 4.5.

consent of the individual to the use or disclosure of that personal information for data matching, it cannot be used or disclosed for data matching.

However, these limitations on collection, use and disclosure are not as strong as might initially appear. Section 7 of *PIPEDA* describes a series of situations where organizations can collect, use and disclose personal information without the consent of the individual. For example, an organization may collect personal information without the knowledge or consent of the individual for the purpose of making a disclosure:

- that is required by law;
- to a government institution that has made a request for the information, identified its lawful authority to obtain the information and indicated that it suspects that the information relates to national security, the defence of Canada or the conduct of international affairs; or
- on the initiative of the organization to an investigative body, a government institution or a part of a government institution and the organization suspects that the information relates to national security, the defence of Canada or the conduct of international affairs.[16]

In short, section 7 allows organizations to act as agents of the state by collecting information, without consent, for the sole purpose of disclosing it to government and law enforcement agencies. Thus, an organization subject to *PIPEDA* could collect, use and disclose personal information from an identity document that it is not justified in collecting, using or disclosing for its own purposes, as long as these actions serve the government interests identified immediately above.

Like the *Privacy Act*, *PIPEDA* gives the Privacy Commissioner no direct powers of enforcement. The Commissioner is an ombudsman. However, the

[16] Section 7(1)(e).

Commissioner can under *PIPEDA* take some complaints to the Federal Court, which does have powers of enforcement.

One means to prevent organizations from ignoring *PIPEDA* might be a specific, enforceable prohibition against collecting, using or disclosing "extraneous" personal information contained in identity documents – for example, a bar owner capturing the additional information contained on a driver's licence that has been used as proof of age of majority. This would prohibit organizations from attempting to capture personal information from government-issued documents in order to profile individuals, and it would penalize those who do. The Ontario *Personal Health Information Protection Act, 2004*[17] provides an example of such an approach. The Act prohibits a person who is not a health information custodian from collecting or using another person's health number except for certain purposes set out in that Act. Violating this prohibition can result in a fine of up to $250,000.[18]

Data protection legislation appears to offer greater protection against the misuse of identity systems by the private sector than it does against the misuse of these systems by the federal government. However, the *Charter of Rights* could limit the actions of the federal government, while it would not apply to the private sector.

**Reviewing existing identity systems:** Parliament should also review the design of existing identity systems (through "identity management impact assessments," which could be similar to today's "privacy impact assessments") to determine their goals, and whether those goals are justifiable. Even if the goals are justifiable, Parliament should limit privacy intrusions associated with identity systems to those that are *necessary* to achieve the goals. In addition, intrusions must be reasonable and proportionate. In some cases, that may involve the

[17] S.O. 2004, chapter 3, section 34.
[18] *Ibid*, section 72.

government in promoting or accepting measures that permit individuals to remain anonymous in certain situations if they choose.

**Respecting Anonymity as the Norm**: Parliament should promote anonymity as the norm in law. If a government institution can show why anonymity is not appropriate, it should nonetheless, through legislation or technology, limit inappropriate data matches and also limit the use of unnecessarily intrusive authentication requirements. In many situations where all that is needed is proof of entitlement or authorization, identity systems should reflect this, and government should promote this principle. Legislation may be the only effective approach, particularly since it would force organizations to consider the privacy implications of their identity initiatives.[19]

**Defending privacy in international relations**: At the international level, the federal government must challenge demands by other governments and international bodies for identification requirements that are unnecessarily intrusive according to Canadian privacy standards. The federal government has a limited ability to influence the identity requirements imposed by other governments and international organizations, but it should not shy away from asserting privacy values at the international level.

**Introducing a "technology principle":** Protecting privacy in identification management requires more than technical measures such as "tokens" attesting that someone is authorized to do (for example, drive a car) or receive something (for example, publicly funded health care). It also requires legal and policy principles to bolster those technical measures. This can be achieved by adopting

19 Office of the Information and Privacy Commissioner/Ontario and the Registratierkamer, The Netherlands, Privacy-Enhancing Technologies: The Path to Anonymity (Volume I), August 1995: "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."

a principle that states that identity system designs must provide the least information necessary to achieve the justifiable purposes of the system. Industry should then bear the burden of proving that it is complying with the principle, through "identity management impact assessments."

That said, there is a very real practical problem with such assessments at this time. There is no equivalent for identity systems to the quality assurance processes that are available in other environments (ISO 9000, for example). There is therefore no mechanism by which an organization can be assured that a particular identity system being touted by a vendor is truly privacy-enhancing or privacy friendly.

In the interim, a four-part reasonableness test might be the appropriate way for organizations to address the issue:

- Is the identity measure demonstrably necessary to meet a specific need?
- Is it likely to be effective in meeting that need?
- Is the loss of privacy proportional to the benefit gained?
- Is there a less privacy-intrusive way of achieving the same end?

The fair information principles behind data protection legislation the world over were drafted in the era of paper records. Important elements of the principles are outdated in light of the advances in technology since the principles appeared in 1980.[20] In particular, the principles should be updated by a "technology" principle that recognizes the power of technology to intrude, and that in particular stresses the need for a strong justification for correlating identifiers contained in separate databases. This would in essence simply be a generalization of the kinds of laws that many countries have for social security numbers.

[20] *OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data* (1980).

**Promoting technological solutions:** Just as technology has created the capacity for ever-greater surveillance, technology can limit that surveillance. As Dr. Stefan Brands notes:

> [I]dentification and privacy are not opposite interests that need to be balanced: the same technological advances that threaten to annihilate privacy can be exploited to save privacy in an electronic age.[21]

This view is echoed in a 2005 UK study:

> Technologies such as digital credentials, privacy-friendly blacklist screening, minimal disclosure proofs, zero-knowledge proofs, secret sharing, and private information retrieval can be used as building blocks to design a national ID card that would simultaneously address the security needs of government and the legitimate privacy and security needs of individuals and service providers. The resulting ID card would minimise the scope for identity theft and insider attacks. ... These solutions are well known to the private sector, but are rarely sought out when governments endeavour to develop national identification systems.[22]

A discussion of the many technological means to protect identity is beyond the scope of this paper. Suffice it to say that the challenge is the struggle that will be involved in getting government support for identification systems that incorporate these technological means to protect privacy.

**Public Education**: Individuals need to understand the role of identity in shaping their privacy. Education is key, but it must be education that can be understood,

[21] Stefan Brands, "Secure User Identification Without Privacy Erosion," (2006) 3:1, University of Ottawa Law & Technology Journal 205-223, http://www.uoltj.ca/articles/vol3.1/2006.3.1.uoltj.Brands.205-223.pdf

[22] Department of Information Systems of the LSE (editor), "The Identity Project: an assessment of the UK Identity Cards Bill and its implications", London, Version 1.09, June 27, 2005.

not merely by technical experts, but by the public at large. As noted earlier, that is one of the main goals of this paper – to help readers understand some of the basic tenets of identity systems so that they can contribute to the debate about shaping policies and laws on identity. A better understanding of the privacy impact of identity systems is particularly important at a time when security concerns are leading to calls for increasingly intrusive identification methods, and are also making the assertion of the right of anonymity suspect.

Governments wanting to introduce identity systems to respond to their concerns about crime and national security should not downplay the privacy consequences of such systems. However, because governments are likely to downplay the privacy implications, the public must have other sources of information to help it understand the privacy consequences of various identity measures.

## Conclusion

Identity management should provide mechanisms for establishing identity, authorization or entitlement according to the following broad privacy rules. It should:

- As a general rule, have the goal of maximizing privacy of the individual consistent with the legitimate needs of government or private sector organizations for proof of identity, authorization or entitlement;
- Allow anonymity as the default position;
- Require identification only when necessary for a legitimate government or business purpose, and when other, less intrusive, measures will not accomplish the same goal. This should be made a legal principle, with "burden of proof" and "identity management impact assessments" in support;
- Enable governments to administer their responsibilities effectively, including responsibilities for the following:
    - Security of citizens (protection from crime, fraud)
    - Administering benefits programs
    - Providing documents attesting to the identity of individuals.

As one co-author[23] of a report[24] on surveillance noted at the 2006 International Data Protection and Privacy Commissioners' Conference, we already live in a surveillance society (his remarks pertained to the United Kingdom, but could largely pertain to other Western countries as well.). All the surveillance tools that

[23] Dr. David Murakami Wood, address to the 28th International Data Protection and Privacy Commissioners' Conference, London, UK, November 2, 2006.
[24] *A Report on the Surveillance Society,* For the Information Commissioner by the Surveillance Studies Network, September 2006: http://www.ico.gov.uk/upload/documents/library/data_protection/practical_application/surveillance_society_full_report_2006.pdf (accessed May 31, 2007).

would be useful for an authoritarian society are now in place, he said. He reminded delegates how easy it is to slip into extensive social control once powerful technologies of surveillance are present. In other words, the tools that are available for surveillance in a democratic society can very easily be put to work in an authoritarian society. We must always keep this in mind when designing policies and systems, including identity policies and systems.

One unspoken concern about various identification systems now under consideration is the one-way nature of rights protections. Governments do not want to appear "soft" on terror. They do not want to appear soft on crime. They are tempted to reach for measures, including intrusive identification systems, that will address or appear[25] to address terror, crime and inefficiency, all the while downplaying, ignoring or remaining ill-informed about the privacy concerns raised by such schemes.

Once an intrusive power is introduced with the goal of attacking terrorism or crime, it is unlikely to be abandoned, even if it proves to be entirely ineffective in achieving its goals. Rights, including privacy, once lost, are not easily regained. This is the phenomenon of the "one-way door."[26] Institutionally, there are too many advantages to preserving intrusive schemes (even if they ill-serve the individual citizen) and, politically, there are too many disadvantages to abolishing them. Even the courts applying the *Charter of Rights* may be reluctant to challenge the actions of governments in times of perceived crisis – just the times when the oversight of the courts is most important.

That is why there is so much need to "get it right" on identity.

[25] Some describe this process of adopting measures that give the illusion of providing greater security as "security theatre."
[26] However, the UK did abandon its wartime ID card system for aliens in 1952: Privacy International, Interim Report: Mistaken Identity; Exploring the Relationship Between National Identity Cards & the Prevention of Terrorism (April 2004) at 3.

# Appendix A: The National Identity Card Debate

Among the identity issues receiving the most public attention in recent years has been the merits of a national identity card. Discussion occurred in earnest in the United States after the September 11, 2001, terrorist attacks there. In Canada, the former Minister of Immigration and Citizenship convened a forum on biometrics in Ottawa in October 2003 "to look at the use of biometrics in the context of measures to enhance the integrity of identity and travel documentation for Canadian citizens and permanent residents." The Standing Committee on Citizenship and Immigration also issued an interim report on a national identity card in October 2003. The report concluded:

> It is clear that this is a very significant policy issue that could have wide implications for privacy, security and fiscal accountability. Indeed, it has been suggested that it could affect fundamental values underlying Canadian society. A broad public review is therefore essential. The general public must be made more aware of all aspects of the issue, and we must hear what ordinary citizens have to say about the timeliness of a national identity card. We hope that this document will stimulate further thought and we encourage Canadians to continue to forward their views to the Committee.[27]

Describing the discussion as being about a national identity *card* presents too simplistic a picture of the issue. What is involved is a national identity *system*, involving mechanisms for proving the identity of the individual, capturing biometrics relating to the person, developing a tamper-resistant "card,"

[27] House of Commons Canada, "A National Identity Card for Canada? Report of the Standing Committee on Citizenship and Immigration" (Interim) (Joe Volpe, MP, Chair), October 2003 at p. 28. http://www.parl.gc.ca/InfocomDoc/Documents/37/2/parlbus/commbus/house/reports/cimmrp06/cimmrp06-e.pdf.

establishing a secure database that can serve legitimate security functions and be accessed by multiple agencies, appointing a bureaucracy to administer the system, incorporating security measures to prevent unlawful access to the database relating to the system, looking at means to prevent the subversion of the system by technical intrusions or corruption of individuals working with the system, developing "readers" to read the cards, and addressing many non-privacy-related issues, such as cost.

Successive Privacy Commissioners of Canada have stated their concerns about a national identity card. Among the concerns they have raised are the following:

- National ID cards are claimed to be an effective way to fight terrorism. Precisely how an ID card would combat terrorism is not clear;
- Anyone arguing that privacy must be diminished in the interest of protecting against crime and terrorism or easing our passage across borders bears an extremely heavy burden of proof. The burden should fall on those who call for a national ID system to explain its benefits in terms of:
    - Added security
    - Protection of other liberties
    - Minimal interference with privacy
    - Being the least intrusive option consistent with achieving the legitimate goals of the system;
- A national ID system may increase the risk to national security, rather than decrease it. The existence of the system may create a false sense that security issues have been addressed, when in fact many security issues have little or nothing to do with identity. In addition, good security requires "depth" of security – multiple means of protecting security. To the extent to which a national identity card might give comfort that such "depth" is not necessary, it might increase threats to security. Conversely, the evidence that a national ID card would increase security is lacking;

- Criminals and terrorists will focus their efforts on subverting the national ID system, since a fraudulent card issued using the system will provide "bullet-proof" identity. The system might be compromised by technical means (as with Canada's Maple Leaf Card) or by corrupting public officials. The system will also become an important target for identity thieves because of the array of personal information contained in its databases;
- The fact that someone possesses a national ID card offers little assurance that the individual is not a terrorist or criminal. Many of those involved in recent terrorist attacks in the United States and the United Kingdom had legitimate identification documents and could obtain legitimate documents under a national identity scheme;
- Some will simply not bother with identification, and will simply sidestep the issue, as do many illegal immigrants generally;
- A national ID system, depending on its structure, could provide the common linkage for numerous databases. In other words, a national ID system might provide a common identifier that would enable disparate databases to be linked, creating a comprehensive profile of an individual. There is nothing intrinsically wrong with establishing our identity every time we make a credit card purchase, rent an apartment, board an aircraft, cross a border, pay our taxes, or negotiate a loan. However, linking all those transactions by use of the same identifier is an entirely different matter. Indeed, a national ID system raises the possibility that the state or private sector organizations may create or have access to massive databases on every individual, detailing information on some of the most personal aspects of their lives, without their knowledge or consent;
- The creation of a biometric national identity card, as it is used for more and more purposes, would also open the door to relentless tracking of the activities, transactions and whereabouts of individuals;
- In its essence, the privacy problem with national identification cards is that they allow us to be identified when we have every right to remain

anonymous, reveal more information about us than is strictly required to establish our identity or authorization in a particular situation, and allow our various activities to be linked together to form patterns and profiles of our lives. Identity cards do not always do this, they do not have to, and it is conceivable that they could be carefully designed and structured so as to avoid it. But it is what they can do, and what they are likely to do;

- A national identification card would radically change Canadian society by drastically infringing on the right to anonymity that is a key part of our right of privacy;
- There is no realistic possibility that such a card could remain voluntary. Even if possessing such a card were made voluntary initially, it would eventually become compulsory, or at least give grounds for suspicion and further inquiry by the state if a person refused to obtain or produce it. This will lead to loss of the opportunities we now have now to be anonymous in society. "Identification creep" will almost certainly occur. As the UK Information Commissioner, Richard Thomas, has suggested, a national ID card could lead to the situation "where the highest level of identity validation becomes the norm for the most mundane of services." Failure to have an ID card, even if the card is voluntary, may lead to second-class service by the private sector, including denial of service in some cases. A national ID card could effectively become an internal passport;
- Function creep **–** finding new uses for information collected for a specific purpose – is a major concern. There will be great temptation to use a national ID card infrastructure for new purposes – for example by adding health data to the ID card chip, or to otherwise combine information in the national ID system with other databanks. The history of the Social Insurance Number (SIN) reminds us that new and unrelated uses will be found. Such a scenario has profound privacy implications, since it holds the prospect of more and more personal information being stored on the card and of transaction data being automatically recorded, logged, transmitted, and used in endlessly creative ways by more organizations.

For example, the bar code on drivers' licences, useful for helping to speed up roadside checks by police officers, yields much more than one's birth date when scanned by a bar or club reader to verify age;

- Depending on the structure of the card, it might be readable by many others, including the private sector (*PIPEDA* and its provincial counterparts would apply to the collection, use and disclosure by organizations engaged in commercial activities in Canada, but there still would be a risk of improper collection for profit);
- Developing a national ID system could be prohibitively expensive, reducing the funds that might be available for other, more productive but less intrusive security measures;
- Even minor error rates in producing the cards could result in large numbers of people being mislabeled;
- Proving (authenticating) one's identity in the first place to obtain a card will be time-consuming and burdensome. In some cases, it may prove impossible for individuals to locate the "foundation" documents such as birth and citizenship certificates that would be needed to prove identity – for example, if documents are stolen or lost in a fire, or if they are located in a third country;
- The technology needed to operate a national ID system may be flawed and, in any event, will need to be updated regularly (at the very least, to stay ahead of those who would want to compromise the system). The fact that Canada is a constitutional federation only adds a further layer of complexity to such a proposal, as provincial and territorial governments would need to be involved in the system's design and operation;
- Any such proposed measure must meet a four-part test of necessity, effectiveness, proportionality and lack of a less privacy-invasive alternative.

# Appendix B: Identity Management Impact Assessments

The following policy and technical questions and issues can serve as a starting point for an assessment of the privacy implications of current or proposed identity systems. The questions and issues have been drawn directly from or are based on the 2002 report of the Computer Science and Telecommunications Board, *IDs – Not That Easy: Questions About Nationwide Identity Systems*. These questions and issues will not be relevant for every identification system, but can nonetheless serve as a guide. In addition, readers might examine the recommendations about authentication contained in *Who Goes There? Authentication Through the Lens of Privacy*.[28] These are set out in part at the end of this Appendix.

### Policy questions

- What is the purpose of the system?
- What is the scope of the population that would be issued an ID and, presumably, be recorded in the system? How would the identities of these individuals be authenticated?
- What is the scope of the data that would be gathered about individuals participating in the system and correlated with their national identity? Would these data be identity data only (and what is meant by identity data)? Or would other data be collected, stored, and/or analyzed as well? With what confidence would the accuracy and quality of this data be established and subsequently determined?
- Who would be the user(s) of the system (as opposed to those who would participate in the system by having an ID)? One assumption seems to be that the public sector/government will be the primary user, but what parts of the government, in what contexts, and with what constraints? In what setting(s) in the public sphere would such a system be used? Would state and local governments have access to the system? Would the private sector be allowed to use the system? What entities within the government

[28] Stephen T. Kent and Lynette I. Millett, *Editors*, Committee on Authentication Technologies and Their Privacy Implications, National Research Council (Washington, D.C., The National Academies Press, 2003).

or private sector would be allowed to use the system? Who could contribute, view, and/or edit data in the system?

- What types of use would be allowed? Who would be able to ask for an ID, and under what circumstances? Assuming that there are datasets associated with an individual's identity, what types of queries would be permitted (e.g., "Is this person allowed to travel?" and "Does this person have a criminal record?"). Beyond simple queries, would analysis and data mining of the information collected be permitted? If so, who would be allowed to do such analysis and for what purpose(s)?

- Would participation in and/or identification by the system be voluntary or mandatory? In addition, would participants have to be aware of or consent to having their IDs checked (as opposed to, for example, allowing surreptitious facial recognition)?

- What legal structures protect the system's integrity as well as the data subject's privacy and due process rights, and determine the government and relying parties' liability for system misuse or failure?

**Technical Issues**

- Plans for design, fabrication, distribution, and updating or otherwise maintaining cards or card readers;

- Plans for design of corresponding databases; the degree of centralization of the underlying databases as well as the location and cost of data storage, computation, and communication. For example, how would authorized entities obtain the records they wanted, under what circumstances, and with what degree of authorization? Would there be daily or weekly downloads of selected records to more permanent storage media?

- Procedures for checking the authenticity of IDs and for verifying the individual presenting the ID;

- Design of means to discover, report, verify, and authoritatively correct mistakes;

- Design of security measures to ensure that the ID system meets its objectives and is not vulnerable to events such as fraud or denial-of-service abuses that can result in privacy violations;

- Determination of need for a real-time network feed (perhaps similar to those used in real-time credit authorization systems) and whether one could reliably secure such a feed.

From *Who Goes There? Authentication Through the Lens of Privacy*:

> There are ways to lessen the impacts on privacy that authentication systems have. Guidelines include the following:
>
> Recommendation: When designing an authentication system or selecting an authentication system for use, one should
>
> - Authenticate only for necessary, well-defined purposes;
> - Minimize the scope of the data collected;
> - Minimize the retention interval for data collected;
> - Articulate what entities will have access to the collected data;
> - Articulate what kinds of access to and use of the data will be allowed;
> - Minimize the intrusiveness of the process;
> - Overtly involve the individual to be authenticated in the process;
> - Minimize the intimacy of the data collected;
> - Ensure that the use of the system is audited and that the audit record is protected against modification and destruction; and
> - Provide means for individuals to check on and correct the information held about them that is used for authentication.
>
> More generally, systems should be designed, developed, and deployed with more attention to reconciling authentication and privacy goals. . . .
>
> Recommendation: In designing or choosing an authentication system, one should begin by articulating a threat model in order to make an intelligent choice among competing technologies, policies, and management strategies. The threat model should encompass all of the threats applicable to the system. Among the aspects that should be considered are the privacy implications of the technologies.

# Glossary

**Attribute** – information of any type relating to an individual. "An attribute describes a property associated with an individual."[29]

**Authentication (and authenticator)** – the process of providing evidence to support a claim about identity. For example, a birth certificate can be used as evidence to support a person's claim about their place of birth. The birth certificate is an "authenticator," or item that helps prove the claim. "An authenticator is evidence that is presented to support the authentication of a claim. It increases confidence in the truth of the claim."[30]

**Biometrics** -- the automatic identification or identity verification of individuals on the basis of behavioural or physiological characteristics.[31]

**Breeder document/credential** – document that is used to obtain other documents used for identity.[32] A birth certificate may be used to obtain a passport. The birth certificate is the "breeder" document/credential. The passport is the identity document. Note that the breeder document/credential – in this case, a birth certificate – can also be considered an identity document.

**Common Identifier** – usually a number (such as a Social Insurance Number) that is used in several databases as the basis ("index") for recording information – in this case, information about an individual. Where several databases use a common identifier such as a Social Insurance Number, correlating the information contained in those databases is very simple. The use of common identifiers across several databases permits the development of profiles of individuals' behaviour, based on the information brought together from those databases.

**Computer matching** – see "data matching."

**Credential** – a piece of information attesting to the integrity of certain stated facts. Credentials are primarily used in the process of authentication, and are then often incorporated in an authentication token – for example, a smart card or bank card.[33]

---

[29] Stephen T. Kent and Lynette I. Millett, *Editors*, Committee on Authentication Technologies and Their Privacy Implications, National Research Council, *Who Goes There? Authentication Through the Lens of Privacy* (Washington, D.C., The National Academies Press, 2003).
[30] Ibid.
[31] Ibid.
[32] http://www.ssa.gov/history/reports/ssnreportc4.html (accessed March 5, 2007).
[33] https://www.cosic.esat.kuleuven.be/modinis-idm/twiki/bin/view.cgi/Main/GlossaryDoc (accessed March 5, 2007).

**Database** – collection of information. Some databases, such as many of those used in identity matters, contain personal information.

**Data matching** – the computerized comparison of two or more sets of records which relate to the same individual. Data matching is likely to involve matching personal records compiled for unrelated purposes.[34]

**Encryption** – the conversion of data into a form, called a ciphertext, that cannot be understood by unauthorized people. Decryption is the process of converting encrypted data back into its original form, so it can be understood.[35]

**Identification** – the process of determining to what identity a particular individual corresponds.[36]

**Identifier** – A "data-item" that is used to distinguish one individual from another. Examples include a person's commonly-used name, or some kind of organization-imposed "username" or code;[37] the name or sign by which a person is known.[38] "An identifier points to an individual. An identifier can be a name, a serial number, or some other pointer to the entity being identified."[39]

**Identity** – Any set of attribute information pertaining to an individual that is stored as a unit. Examples are profiles, records and accounts.

**Identity policy** – the policy surrounding the appropriate role for various means of identifying or authorizing individuals.

**Identity theft** – occurs when an individual assumes the identity of another person and carries out transactions in the other person's name. Identity theft occurs when someone else can bypass/fool an authentication system – for example, because the system uses insufficiently strong authenticators.

---

[34] Simon Rogerson, originally published as ETHIcol in the IMIS Journal Volume 7 No 1 (Febuary 1997): http://www.ccsr.cse.dmu.ac.uk/resources/general/ethicol/Ecv7no1.html (accessed March 5, 2007).

[35] http://searchsecurity.techtarget.com/sDefinition/0,290660,sid14_gci212062,00.html (accessed March 5, 2007).

[36] Stephen Kent and Lynette Millett, eds., National Academy of Sciences, Computer Science and Telecommunications Board, *IDs – Not That Easy: Questions About Nationwide Identity Systems* (Washington, DC: National Academy Press) 2002. at p. 12.

[37] Roger Clarke, "Identification and Authentication Fundamentals" (Version of May 8, 2004): http://www.anu.edu.au/people/Roger.Clarke/DV/IdAuthFundas.html (accessed on April 10, 2006).

[38] Stephen Kent and Lynette Millett, eds., National Academy of Sciences, Computer Science and Telecommunications Board, *IDs – Not That Easy: Questions About Nationwide Identity Systems* (Washington, DC: National Academy Press) 2002.

[39] Stephen T. Kent and Lynette I. Millett, *Editors*, Committee on Authentication Technologies and Their Privacy Implications, National Research Council, *Who Goes There? Authentication Through the Lens of Privacy* (Washington, D.C., The National Academies Press, 2003).

**Phishing** – a technique for defrauding individuals by misrepresenting the identity of an organization to those individuals, usually over the Internet. (Phishing is the electronic version of "pretexting." For example, a fraudster may send an email to the customer of a bank, fraudulently identifying the email as coming from the bank. The email will request the individual to send account and password information to what appears to be the legitimate bank's web site, but which is in reality the web site of the fraudster. The fraudster will use the information that the unsuspecting individual had sent to the "bank" to get access to the individual's bank account.

**Profiling** – the practice of collecting and analyzing data related to an individual with the aim of creating a profile.[40]

**Root document** – A "root" credential is a specific breeder credential, in that it is not obtained on the basis of showing other breeder credentials. It is, in essence, the start of the "chain". See also "breeder document."

**Token** – a token can be a bank card, bus ticket or any other object that is used to show entitlement to a service (a bus token authorizes the holder to ride a bus) or carry out a transaction. A token can be seen as something – tangible or intangible/electronic – that enables a transaction. "A token is any hardware or software that contains credentials related to attributes. Tokens may take any form, ranging from a digital data set to smart cards or mobile phones. Tokens can be used for authorization purposes ("authorization tokens")."[41]

[40] https://www.cosic.esat.kuleuven.be/modinis-idm/twiki/pub/Main/GlossaryDoc/modinis.terminology.paper.v2.01.2005-11-23.pdf (accessed March 6, 2007).
[41] https://www.cosic.esat.kuleuven.be/modinis-idm/twiki/bin/view.cgi/Main/GlossaryDoc (accessed March 5, 2007).