COMMISSION DE L'ÉTHIQUE DE LA SCIENCE ET DE LA TECHNOLOGIE

POSITION STATEMENT

IN SEARCH OF BALANCE

AN ETHICAL LOOK AT NEW SURVEILLANCE AND MONITORING TECHNOLOGIES FOR SECURITY PURPOSES

Québec

COMMISSION DE L'ÉTHIQUE DE LA SCIENCE ET DE LA TECHNOLOGIE

POSITION STATEMENT

IN SEARCH OF BALANCE

AN ETHICAL LOOK AT NEW SURVEILLANCE AND MONITORING TECHNOLOGIES FOR SECURITY PURPOSES

COMMISSION DE L'ÉTHIQUE DE LA SCIENCE ET DE LA TECHNOLOGIE

POSITION STATEMENT

IN SEARCH OF BALANCE

AN ETHICAL LOOK AT NEW SURVEILLANCE AND MONITORING TECHNOLOGIES FOR SECURITY PURPOSES

Québec

COMMISSION DE L'ÉTHIQUE DE LA SCIENCE ET DE LA TECHNOLOGIE

1200 Route de l'Église
3rd Floor, Office 3.45
Québec (Québec)
G1V 4Z2
www.ethique.gouv.qc.ca

Production support

Coordination and supervision

Diane Duquet and Nicole Beaudry

Meeting secretary

David Boucher

Research and writing

David Boucher and Diane Duquet

Technical support

Secretary

Annie St-Hilaire

Documentation

Monique Blouin and Annie Lachance

Communications and editing supervision

Guillaume Huet

Cover Design

Création Sylvain Vallières Inc.

Design and layout

Éditions MultiMondes

Translation

Ross & Sheehan Inc.

Position statement adopted at the 34th meeting of the Commission de l'éthique de la science et de la technologie
February 12th, 2008

Dépôt légal: 2008
Bibliothèque nationale du Québec
National Library of Canada
ISBN 978-2-550-52629-2

Members of the Working Committee

President

BENOÎT GAGNON
Associate Researcher
Canada Research Chair in Security,
Identity and Technology
Doctoral Candidate at Université de Montréal

Members

FRÉDÉRIC ABRAHAM
Doctoral Candidate
Université du Québec à Trois-Rivières

PATRICK BEAUDIN
Director General
Société pour la promotion de la science
et de la technologie

ÉDITH DELEURY
President, CEST
Faculté de droit
Université Laval

BENOÎT DUPONT
Chairholder, Canada Research Chair in Security,
Identity and Technology
Professor
École de criminologie
Université de Montréal

FRÉDÉRICK GAUDREAU, Lt
Coordinator
Module de la cybersurveillance et de la vigie
Sûreté du Québec

STÉPHANE LEMAN-LANGLOIS
Researcher
Centre international de criminologie comparée (CICC)
Professor
École de criminologie
Université de Montréal

DANIELLE PARENT
Directrice des affaires juridiques
Bureau du Commissaire au lobbyisme du Québec

MARIE-CLAUDE PRÉMONT
Law Professor
École nationale d'administration publique (ÉNAP)

SERGE TRUDEL
Director, Access to Information/Ethics
Canadian security Association (CANASA)

DANIEL MARC WEINSTOCK
Chairholder, Canada Research Chair in Ethics and
Political Philosophy
Professor
Département de philosophie
Université de Montréal

Observing Member

RAYMOND D'AOUST
Assistant Privacy Commissioner of Canada

From the Commission secretariat

Nicole Beaudry, CEST Coordinator
David Boucher, Ethics advisor

Conseil de la science et de la technologie
Québec

Québec, le 3 mars 2008

Monsieur Raymond Bachand
Ministre
Ministère du Développement économique, de l'Innovation et de l'Exportation
710, place d'Youville, 6e étage
Québec (Québec) G1R 4Y4

Monsieur le Ministre,

Je vous transmets par la présente la version finale de l'avis intitulé Viser un juste équilibre : *Un regard éthique sur les nouvelles technologies de surveillance et de contrôle à des fins de sécurité*, préparé par la Commission de l'éthique de la science et de la technologie.

Espérant le tout à votre entière satisfaction, je vous prie d'accepter, Monsieur le Ministre, l'expression de ma haute considération.

La présidente,

Marie-France Germain

Commission
de l'éthique
de la science
et de la technologie
Québec

Québec, le 3 mars 2008

Madame Marie-France Germain
Présidente
Conseil de la science et de la technologie
1200, route de l'Église
3e étage, bureau 3.45
Québec (Québec) G1V 4Z2

Madame la Présidente,

Il me fait plaisir de vous remettre l'Avis au ministre du Développement économique, de l'Innovation et de l'Exportation intitulé *Viser un juste équilibre : Un regard éthique sur les nouvelles technologies de surveillance et de contrôle à des fins de sécurité*.

Je vous prie de recevoir, Madame la Présidente, mes salutations distinguées.

La présidente de la Commission de l'éthique
de la science et de la technologie,

Édith Deleury

Table of Contents

List of acronyms

AAPI:	*Association sur l'accès et la protection de l'information*
DNA:	Deoxyribonucleic acid
CAI:	*Commission d'accès à l'information* (Québec)
CANASA:	The Canadian Security Association
CCNE:	*Comité consultatif national d'éthique pour les sciences de la vie et de la santé* (France)
CNIL:	*Commission nationale de l'informatique et des libertés* (France)
RFID:	Radio Frequency Identification
NSMT:	New Surveillance and Monitoring Technologies
OECD:	Organisation for Economic Co-operation and Development
UN:	The United Nations

Summary and recommendations

Mass surveillance can be considered a fact of modern society. Its significance is reflected in the variety of methods used to collect information. Among these methods, New Surveillance and Monitoring Technologies (NSMT), and particularly the way in which they are used, raise a number of ethical issues. In addition, the *Commission de l'éthique de la science et de la technologie* has taken on the mandate of formulating a Position statement on technology which could be used in mass surveillance for purposes of security: Biometric systems, video surveillance and radio-frequency identification (RFID).

The Commission wished to consider specifically those NSMT as they are applied towards purposes of security, excluding workplace surveillance, health-related uses and inventory management applications. But what does security mean? Merely asking the question raises the concept's complex nature. In fact, not only does the term evoke a variety of meanings, particularly at the sociological level, but its very interpretation also varies among languages, views, approaches and history.

Providing security for a territory, a country, city, or home is a constant challenge which involves accurate threat assessment and the implementation of effective protection systems. Today, and especially since the events of September 11th, 2001, entirely new threat and security issues have emerged and would seem to require the implementation of equally new measures at both the technical and political levels. NSMT figure among these new measures.

The Commission, wishing to consider the issues from a broader social, political and ethical context, began its reflection by questioning the potential links between NSMT deployment and feelings of insecurity with regards to crime, and the increasing importance given to issues of risk and surveillance.

First of all, the Commission wished to explore the sense of insecurity frequently reported by the media. It would appear, in fact, that how people feel about their own security depends on many factors, and could be influenced by a variety of players, which makes the issue rather difficult to define. In order to better evaluate the true scope of this sense of insecurity, the Commission has examined several studies and investigations on the subject. According to this analysis, it can be concluded that Canadians and Quebecers feel safe. The amount of media coverage pertaining to crime and terrorism does not reflect the public's concern as reported in these studies. In addition, a strong fear of crime is in contradiction with crime statistics, at least in Canada, which currently report a decrease in the overall crime rate.

A society driven by insecurity, willingly or not, is more inclined to constantly seek information to assess and manage potential risks and dangers. Several thinkers feel that this obsession with risk, threats and danger is a symptom of the insecurity that affects a society. This is in fact why authors such as sociologist Ulrich Beck qualify these societies as risk societies. Among risk societies' various characteristics, the need for information on the part of leaders as well as their citizens is particularly relevant to this Position statement. According to risk society theorists, the more information people have at their disposal, the better they can calculate, analyze and manage risks in the hopes of reducing or eliminating them. In applying this principle to the realm of security, it seems obvious that NSMT represent a powerful means of collecting information that can be used to thwart security threats and reduce crime. Although these principles cannot fully account for the appeal of NSMT, the Commission believes they nevertheless act as a driving force behind the deployment of NSMT for security purposes.

Information gathering is absolutely vital to risk societies. This information is obtained by surveillance, among other means. Surveillance, however, is not a new phenomenon, and it did not await the advent of risk societies or advanced technology to emerge. Surveillance has been an integral part of human civilization since

time immemorial, as even socialization itself would be unthinkable without adult supervision. Recently, and especially since the terrorist attacks of September 11th, 2001, a change in direction can be observed in the methods used to gather information. Surveillance is no longer restricted to what are considered "risk" segments of the population. The general public is now placed under surveillance in order to target actions against individuals considered at risk, or who represent a risk to others.

It is not really the imminent rise of a "Big Brother" that concerns the Commission, but rather the emergence of a number of "Small Brothers", or a number of organizations and individuals who privately conduct surveillance activities for security purposes that is troubling. This type of surveillance, which does not necessarily follow proper guidelines and sound practices could fall completely beyond the control of the state.

Based on these contextual elements, the Commission defines the ethical framework used in its ethical look at NSMT. With regards to values, the Commission wishes to assert its commitment to the fundamental values shared by democratic societies. Autonomy, a central value of these societies, is the value which allows individuals to live their lives as they see fit, within the limits of the rights and freedoms of others. In this Position statement, it is conceived as the expression of freedom by citizens of democratic societies, particularly with regards to the sometimes-intrusive role of the state and other organizations. Moreover, the Commission believes that increased citizen involvement in the design, implementation and follow-up of the various guidelines surrounding NSMT would represent greater compliance with the democratic ideal and respect for autonomy.

The desire to promote individual autonomy among liberal democracies is rendered tangible by a commitment to a whole range of other fundamental values. Although they may conflict in certain cases, it is generally recognized that these values share a common origin. They are the conditions under which autonomy becomes possible, and from that point forward, democracy itself. Among this set of values, the Commission has focused on those most concerned by the deployment of NSMT: Security, freedom, privacy, transparency, justice and equality. In so doing, the Commission highlights the fact that the use of NSMT must never lose sight of its primary objective: To protect democratic societies against the risk of compromise to its fundamental values. The danger lies in the fact that in attempting to provide too much security, surveillance methods can threaten the fundamental values that help define these democratic societies. The Commission, in this Position statement, aims to strike a fair balance between security and individual rights and freedoms in the protection of fundamental democratic values.

On a technical level, the Commission provides a detailed description of the three NSMT under consideration.

A **biometric system** allows a person to be identified, or to verify a person's eligibility "to be given certain rights or services (namely access) based on the recognition of physical attributes (fingerprints, retinal patterns, hand geometry), traces (DNA, blood, odours), or behaviours (signature, gait)[1]". Biometric system applications are for the most part little understood and still rather rare.

Video surveillance involves remote monitoring of public or private areas, using cameras, most often motorized, which transfer images taken from monitoring equipment to be viewed on a screen. This type of surveillance and monitoring technology is much more widely used and familiar. It is unclear, however, that more recent technological advances, such as digitization combined with face recognition software are as commonly known.

Radio-frequency identification (RFID), though not a new technology *per se*, has found rather surprising applications in a variety of areas. RFID involves two main components. First, a tag containing an "electronic circuit that stores data and an antenna which communicates the data via radio waves[2]" is required. This tag then communicates with a

1. Definition by the Commission nationale de l'informatique et des libertés (CNIL – France), as stated in Office parlementaire d'évaluation des choix scientifiques et technologiques, *Les méthodes scientifiques d'identification des personnes à partir de données biométriques et les techniques de mise en œuvre*, Report presented to the Senate by Christian CABAL, (France: Assemblée nationale, June 2003), p. 8, [Translator's note: an summary of this report is available in English at <http://www.palais-bourbon.fr/12/dossiers/030938.asp#PDT>].
2. WORKING PARTY ON THE PROTECTION OF INDIVIDUALS WITH REGARD TO THE PROCESSING OF PERSONNAL DATA OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL OF 24 OCTOBER 1995. *Working document on data protection issues related to RFID technology*. Brussels, 19 January 2005, p. 3. [http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2005/wp105_en.pdf].

reader, which includes "an antenna and a demodulator which translates the incoming analogue information from the radio link into digital data. The digital information can then be processed by a computer[3]". The inclusion of tags containing personal or other information in identity documents or access cards constitutes the main application of RFID in security applications. Since they can be scanned from a remote location, these tags allow for individuals to be traced and documents to be secured so as to prevent fraud and identity theft.

The deployment of NSMT raises several ethical issues. The Commission has selected the following for further analysis.

Assessment of the relevance, effectiveness and reliability of NSMT

In order to ensure their legitimate deployment, the Commission feels that NSMT must be relevant, effective and reliable. To be relevant, NSMT must be determined as the best method of achieving a given security objective. Other means, which are less intrusive to privacy, could thus be favoured. In order for NSMT to be effective, they must produce results that match initial expectations. Furthermore, NSMT must be reliable, that is to say, their operation must never present more problems than solutions. In order to justify their deployment, NSMT must reach higher levels of relevance, effectiveness and reliability. The Commission also wishes to emphasize the importance of deploying effective and reliable technologies to avoid causing harm to innocent people. These questions, though technical, require solutions where public transparency should be a central feature. The assessment of the effectiveness of NSMT must be as transparent as possible in order to ensure public access to accurate information. The Commission also wishes to caution against the deployment of technologies perceived as reliable that would contribute to promoting a false sense of security among the public.

Proportionality of response to insecurity

The Commission is concerned by the potential scale of an NSMT deployment in response to an insatiable demand for security. The use of NSMT must take into account the ethical issues involved, and seek to achieve a level of security deemed acceptable without going overboard. Bridges must therefore be built among the various players involved and the general public in order to come to a consensus.

In concurrence with the *Comité consultatif national d'éthique pour les sciences de la vie et de la santé* (CCNE), the Commission believes that the proportionality of means concept must be taken into consideration, not only with regards to biometric systems, but with NSMT in general. Implementation of surveillance methods that are too intrusive, considering their end purpose and context, just as integrating personal data beyond their declared purpose, would be ethically unacceptable. The Commission calls on decision-makers in both the public and private sectors to conduct a careful and lucid assessment of their needs with regards to NSMT for security purposes.

It is essential that an evaluation of the relationship between technical reliability, proportionality of response to insecurity and the degree of intrusiveness be conducted for each and every NSMT deployment. It appears that such an evaluation would in itself allow for insights into the ethics behind the end purposes to which NSMT are actually implemented. Such a groundbreaking process would undeniably help Québec assume a leadership role in the assessment of the ethics involved in the use of these technologies.

Moreover, at the heart of the assessment of the proportionality of response to insecurity lie players who are all too often ignored by private and public decision-makers: NSMT providers and fitters. These players are on the front line in that they must directly meet the technical security needs of private and public organizations and citizens. In addition to providing appropriate advice to their clients on the use of NSMT, they must be prepared to answer the following question: Which technology is best suited to ensure a given level of security? In other words, which security system is best recommended to meet their security requirements? These providers and fitters are the first to be confronted by the ethical issues raised by the Commission. It is also necessary that they be sensitized to the ethical questions involved in their practices if the deployment of NSMT is to be consistent with the promoted values. The central question appears to revolve around the issue of

3. Ibid.

how to achieve proportionality of response to insecurity in a context of very rapid market growth where an emphasis on profit often overshadows ethics. These considerations suggest a deeper analysis of NSMT regulation. The results could then be distributed among key players through subsequent legislative developments.

In Québec, the new Private Security Act specifically governs "activities related to electronic security systems, namely, installing, maintaining and repairing, and ensuring the continuous remote monitoring of, burglar or intrusion alarm systems, video surveillance systems and access control systems, except vehicle security systems […][4]". The Act further stipulates that the future *Bureau de la sécurité privée* will provide training to representatives of licensed agencies and that the Government could, by regulation, determine which training is appropriate in order to use certain equipment, or which training credentials are required for the deliverance of an agent licence[5]. This training should include a section focused on ethical issues. Hence:

The Commission recommends that training provided by the *Bureau de la sécurité privée* to representatives of licensed agencies include a compulsory ethics component based on the ethical issues raised in this Position statement and that the Government, in compliance with the Private Security Act, adopt the necessary regulations so that the training required for the deliverance of an agent licence also include an ethics component.

Social Acceptability

The true measure of social acceptability of NSMT deployment is difficult to determine. Better knowledge of public perceptions and opinions in this area would certainly help provide further insight into this issue. It is important to gain better knowledge on the public's perspective with regards to NSMT. It is also essential to give a voice to those who will be placed under surveillance in order to ensure that deployment be both acceptable to, and accepted by society.

Considering the current popularity of governments that have made security their key issue and in the light of the results of polls and surveys on public acceptance of NSMT, it would appear that NSMT deployment is not contrary to popular will. The Commission, however, raises questions as to the levels of public awareness with regards to biometrics, video surveillance and radio frequency identification (RFID). Moreover, any form of consultation on NSMT should place a premium on public participation and to seek, above all, to collect informed and enlightened opinions.

Consent

In most cases, it is simply impossible for individuals under surveillance to give their consent. Individual free and clear consent is simply not a concept that can be applied to NSMT. This statement of fact is not, however, above raising questions of ethics.

Biometric data can in fact be collected without a person's knowledge; surveillance cameras can capture images from a downtown street without the consent of passers by, and subcutaneous RFID implants could be impossible to refuse by certain categories of people. Various legal provisions guide the collection and distribution of personal data collected by NSMT. Some of these provisions, however, have limitations. The Commission firmly believes it is necessary to implement means and procedures by which public concerns and complaints could be heard and considered.

Moreover, the Commission feels that the public should be better informed, specifically but not exclusively, with regards to the following points:

- The legal provisions surrounding the deployment of NSMT, the collection, use, and sharing of personal data;
- The risks, disadvantages, advantages and potential benefits of the deployment of NSMT;
- Places and documents brought under surveillance;
- Means available to the public enabling their involvement in the deployment of NSMT, thereby allowing for an open and transparent process.
- Means available to the public to make its opinions on the matter known, including complaints against NSMT in general, or a NSMT deployment plan in particular.

In the spirit of the principle of representation, by virtue of which elected officials make political decisions rather than the public as a whole, the Commission believes that

4. R.S.Q., chapter S-3.5, 2006, c. 23, s. 1.
5. R.S.Q., chapter S-3.5, 2006, c. 23, s. 41, 111 and 112.

if the deployment of NSMT is done in a manner that is transparent and in accordance with the fundamental values of democratic societies, individual consent is not necessarily required. It is essential, however, to bring together conditions that shed light on the process leading to the deployment of NSMT and to give to opponents and critics all the necessary leeway so that they are allowed to voice their point of view.

With regards to the issue of consent, the Commission cautions citizens as to the stealthy nature of NSMT. The goal of many NSMT promoters, in fact, is to blend them into the environment to make them invisible. The Commission believes that this could have repercussions on individual autonomy and privacy.

Respect for the end purpose

Respect for the end purpose to which NSMT are deployed and the exploitation of all other possible uses are a source of tension. On one hand, respect for the stated end purpose is an important principle which tends to prevent diverted use and certain forms of abuse and excess. On the other hand, exploitation of all other possible uses of NSMT (including ends to which individuals have not given their consent) would probably allow for increased security.

Considering the examples brought to its attention, the Commission is concerned about the shifts it has observed and those that could occur in the near future. Standards, procedures, practices, surveillance and monitoring methods implemented after the terrorist attacks have been progressively incorporated into the fight against petty crime, and eventually made their way into the business sector. Conversely, technologies such as RFID, whose applications are most often associated with retail businesses and inventory management, appear to be making their way into the realm of security. Moreover, considering how easily NSMT find a variety of applications and end purposes, a call for vigilance is deemed appropriate.

The storage period for data collected by NSMT constitutes an important element in the risk of function creep. The principle is simple: Shorter data storage periods decrease the likelihood of its use for other purposes. Consequently, it is important to determine a data storage time frame before a surveillance system is implemented, and that it not exceed the normal storage period required to meet the intended purpose.

Finally, the Commission wishes to draw attention to the fact that analyses of personal information collected by NSMT involve risks of discrimination and stigmatization. Given the nature of the personal information collected and the possibility of extracting information on ethnic origin, user health, consumer habits, or affiliation to political parties, questions regarding these issues must be raised. Although surveillance systems are not implemented with the purposes of discrimination and stigmatization, the Commission feels that this type of outcome is as plausible as it is unacceptable.

NSMT do, nevertheless, offer considerable surveillance and risk assessment and management potential for security purposes, a point which should neither be ignored nor underestimated. Although some may see a threat to individual rights and freedoms in the growing popularity of surveillance methods, others with a more optimistic view will point to the crime and terrorism prevention potential of this technology.

On the whole, the risk of abuse and excess stemming from function creep, though possibly helpful in crime prevention or identifying criminals in certain cases, deserves full attention. By allowing the exploitation of all possible uses of NSMT in order to protect democracy and law and order against terrorism and other crimes, the Commission is concerned about compromising the very rights and liberties that constitute the founding principles of democracy. The Commission insists on the necessity to find an appropriate balance, and comes to the conclusion that democracy itself constitutes an ever-delicate balance between freedom and repression. NSMT can do much to help improve public safety, but it is not always necessary to resort to all of their possible applications in order to ensure acceptable safety levels.

Protection of personal information

The question of NSMT is often focused on a single issue: The protection of personal information. This is especially due to the fact that NSMT are essentially deployed to collect information (which is often personal). This issue, more than any other, concerns the value of privacy and security. If on one hand personal information reveals much about the private lives of individuals, it is nevertheless considered a valuable source of information in helping improve security.

The protection of personal information is almost systematically connected to privacy. It is true that information deemed personal opens a window into various aspects of our private lives. In fact, the issue of personal information protection requires an update of the concept of privacy. If personal information protection is primarily a judicial concept, privacy, within the framework of this Position statement must be understood as a value.

The data collected by biometric systems, video-surveillance and RFID almost systematically involve personal information. Consequently, the degree of privacy of those under surveillance will vary according to their use, and how this information is stored and shared.

Protection of personal information is inseparable from biometric systems since biometric measurements are considered personal information. The fact that certain biometric data constitute revealing personal identifiers probably explains why biometric systems cause fear for the worst with regards to individual privacy. Biometric data can be considered personal identifiers as they are intimately related to the individual from whom they were collected. The revealing nature of certain biometric identifiers is also an object of concern: Biometric data contain more information than the simple reproduction of a fingerprint, for example. In fact, according to some experts, it is even possible to collect information on the health or mood of individuals simply by analyzing their fingerprints or retina. People generally prefer that certain information in their possession, and as it pertains to them personally, remain confidential, or at least be treated as such.

Due to its remote and invisible nature, video surveillance can represent a threat to privacy. Technology readily allows for the filming of people without their knowledge in both public and private areas. Therefore, individuals must realize that they do not enjoy the same levels of intimacy in public places as they do in their homes. It would be an exaggeration, however, to expect individuals to completely renounce any right to privacy in public places. Everyone is entitled to expect to be able to move about in public without being the object of constant surveillance. Respect for privacy also applies to public places.

Just as with video surveillance, radio frequency identification (RFID) could become a surreptitious means of surveillance and used to trace and track individuals. For this reason, the Commission's comments with regards to video surveillance apply equally to RFID. The Commission wishes to point out, however, that the nature of the collected information is different. With video surveillance, personal information is collected in the form of images, possibly including faces. In the case of RFID, crucial personal information is likely to be collected: Credit card information, health, identity, nationality, etc. The nature of this information presents a heightened risk to individual privacy.

Considering that new passports issued by most members of the European Union as well as those currently issued to American citizens contain a RFID tag, and given the interest the Government of Canada has shown in incorporating biometric data into identity documents for Canadian citizens, the Commission believes a ruling will soon be needed on how to manage the introduction of this technology into identity documents. Moreover, the European and American experiences demonstrate the importance of adequately protecting personal information if the goal of securing identity documents is to be achieved. For its part, and considering the high levels of risk to privacy and the protection of personal information, the Commission feels it is important that the Québec Government work in concert with Canadian government authorities so that, in the event of the introduction of RFID tags into Canadian identity documents, that the RFID tags containing personal information include an encryption system to secure the data, thereby ensuring better privacy and personal information protection.

It would be unacceptable for decision-making based on automatic data processing to become common practice in surveillance and identity monitoring. Dehumanizing security-related decisions must be avoided. Once again, it appears that a balance must be struck between man and machine with regards to surveillance and data processing. On one hand, the more surveillance systems are managed by people, the more we can expect their life experiences to occasionally influence their decisions. But let us not be deluded: No one can completely set aside their personal views and opinions in the exercise of their work. Moreover, if computerized and automated data processing can reduce the prejudicial influence of surveillance system operators, it remains nonetheless a concern to think that potentially harmful decisions could be taken on the basis of this processing, without anyone having placed this information in its proper context.

Finally, one must question whether the level of protection of personal information is the same from one country to another, and whether the transfer of this information from a country with high levels of protection towards a country with less to offer is acceptable. Consumers are already conducting transactions on the Internet with foreign companies which store their personal information, without any knowledge as to how this information is to be protected. Yet, consumers remain free to abstain from participating in such transactions. But with information obtained through NSMT, individuals are not always aware that their personal information will be stored. Obviously, this raises questions about individuals and their control over the fate of their personal data.

This Position statement brings to light questions to which the Commission is not in a position to provide answers and to which it cannot necessarily follow-up. The Commission does, however, feel that several actions must be taken to find solutions and that the governmental actors who can accomplish them can be readily identified.

Considering that the Minister responsible for Canadian Intergovernmental Affairs, Aboriginal Affairs, Francophones within Canada, the Reform of Democratic Institutions and Access to Information has the mandate to advise the Government by providing position statements with regards to access to information and the protection of personal information, particularly during the tabling of bills or the development of information systems, and that the Commission d'accès à l'information *may be consulted for these purposes;*

Considering that the Commission d'accès à l'information *is responsible for ensuring compliance with, and the promotion of, access to documents and the protection of personal information, and can determine the conditions applicable to a personal information file to which a public body must comply;*

Considering that the Commission d'accès à l'information *can also, after due investigation relative to the collection, retention, disclosure or use of personal information by a person in the course of carrying on an enterprise, and after having given this individual an opportunity to present his observations, recommend or order this person to apply any and all corrective measures required to ensure the protection of personal information;*

And considering that the Commission des droits de la personne et des droits de la jeunesse du Québec *is mandated to:*

- *Design and implement an information and educational program on human rights as well as the protection of children's rights;*
- *Direct and encourage research and publications on fundamental rights and freedoms and on children's rights;*
- *Receive suggestions, recommendations and requests regarding human rights and freedoms, by holding public hearings as needed, and to submit appropriate recommendations to the Government;*
- *Cooperate with any and all organizations devoted to the promotion of human rights and freedoms, both within and outside of Québec,*

The Commission recommends to the Minister responsible for Canadian Intergovernmental Affairs, Aboriginal Affairs, Francophones within Canada, the Reform of Democratic Institutions and Access to Information, the *Commission d'accès à l'information* and the *Commission des droits de la personne et des droits de la jeunesse du Québec* to work together in order to implement the following actions:

1. **Promote a dialogue among citizens, the Government and the industry towards the adoption of guidelines regarding the use of these technologies that take into account the ethical concerns with respect to fundamental democratic values.**
2. **Through a consultative approach, advise the Government with regards to its NSMT deployment projects, particularly in areas which raise ethical issues and according to the criteria of relevance, effectiveness and reliability.**
3. **Organize a public consultation process (based on the model developed by the *Commissaire à la santé et au bien-être*) that would highlight ethical issues.**
4. **Make the results of this consultation publicly available in order to sensitize the general population as to the ethical issues associated with NSMT.**
5. **Inform the general population as to the legal provisions surrounding the deployment of NSMT and its consequences on the values of autonomy, freedom, security and privacy, and the means available to the public to participate in the decision-making, implementation and follow-up processes involved.**
6. **Implement a compensation and correction mechanism for cases where the use of NSMT is prejudicial to individuals by wrongfully associating them with illicit activities.**

Introduction

At its December 9, 2002 meeting, the *Commission de l'éthique de la science et de la technologie* decided to study biometrics as a focus subject in order to render a Position statement. The first step involved the production of a study document and a consultation paper that helped form the basis for a public forum held on October 24th, 2004 on the issues raised by the use of biometric data. This forum was held jointly with the *Raoul-Dandurand Chair of Strategic and Diplomatic Studies* at *Université du Québec à Montréal.* The consultation paper was also used for an online public consultation process where interested parties where invited to submit their comments or papers in order to add further depth and insight to the study.

Following completion of its study of the use of biometric data, the Commission took on the mandate to formulate a Position statement not only on this subject, but on other technologies that could be used in mass surveillance for security purposes: Video surveillance and radio frequency identification (RFID). Following the publication of its Position statement on nanotechnologies, it was deemed important to broaden the theme of biometrics to include new surveillance and monitoring technologies (NSMT), which, while not necessarily dependent on the use of biometric data, are increasingly used for security purposes.

Certain technologies were excluded from consideration, either due to the fact that their complex nature and application deserved separate treatment (cyber surveillance and data mining), or that they only applied to the surveillance of certain individuals (monitoring bracelets). Moreover, the Commission has chosen to consider NSMT as they are applied towards purposes of security, excluding workplace surveillance, health-related uses and applications related to inventory management.

The Commission's mission, among other things, is to help provide direction and guidance to concerned actors in their decision-making process. Since this Position statement focuses on institutional actors, attention is directed towards state-conducted surveillance on citizens as opposed to citizen surveillance on other citizens or the state. These other forms of surveillance, however, are brought into consideration whenever relevant.

The deployment of NSMT is closely related to the social, socio-political ethical and legal context of the modern era. The first chapter outlines this context by calling attention to various points. First, the Commission defines its use of the term "for security purposes" and what it encompasses. The focus then turns to the public sense of insecurity often reported by the media. It turns out that how people feel about their personal safety depends on several factors and could be influenced by various actors. In an attempt to better evaluate the true scope of this sense of insecurity, the Commission has reviewed several studies and investigations on the subject.

Then, considering that NSMT deployment is narrowly connected to the socio-political context of the modern era, the Commission draws attention to the increasing importance given to the assessment, management and elimination of risk. Many thinkers believe that an obsession with risk, threats and dangers is symptomatic of a general insecurity that affects a society. This leads authors such as sociologist Ulrich Beck to qualify these societies as "risk societies".

NSMT are increasingly present in modern everyday life. The Commission, along with other observers, predicts that most modern societies will soon be qualified as "surveillance societies".

From the outset, the Commission defines the ethical framework used in its ethical look at NSMT. It defines the values at stake and outlines the ethical issues that will be presented in the third chapter. With regards to values, the Commission states its commitment to several fundamental values shared by democratic societies. The goal is to reach a fair balance between security and individual rights and freedoms in the protection of the fundamental democratic values.

The main normative texts that set limitations and regulatory terms in this area are also presented, as well as a quick overview of the normative instruments currently in effect in Québec, at the Canadian, regional and international levels.

The second chapter offers a relatively detailed technical description of three NSMT: Biometric systems, video surveillance and radio frequency identification (RFID). A biometric system allows a person to be identified, or to verify a person's eligibility "to be given certain rights or services (namely access) based on the recognition of physical attributes (fingerprints, retinal patterns, hand geometry), traces (DNA, blood, odours), or behaviours (signature, gait)[1]". Biometric system applications are still rather rare. Video surveillance, on the other hand, is a much more widely used and familiar surveillance technology. It is unclear, however, that more recent technological advances, (such as digitization combined with face recognition software) are as commonly known. Finally, radio-frequency identification (RFID), though not a new technology *per se* has found rather surprising applications in a variety of areas. The inclusion of tags containing personal or other information (nationality, sex, date of birth) in identity documents or access cards constitutes the main application of RFID in security applications. Since they can be scanned from a remote location, these tags allow for individuals to be traced and documents to be secured in order to prevent fraud and identity theft.

The Commission takes a specifically ethical look at NSMT and their applications in Chapter 3. In turn, the main ethical issues and cherished values are placed in perspective: The assessment of the relevance, effectiveness and reliability of NSMT, the proportionality of response to insecurity, social acceptability, consent, respect for the end purpose and the protection of personal information.

With this Position statement, the Commission hopes to contribute to and enhance the collective understanding of ethical considerations regarding NSMT deployment, and to offer the decision makers direction and guidance that take into consideration the ethical issues and the fundamental values of democratic societies. In a debate where protagonists hold very divided views, this Position statement strives to be as objective and balanced as possible. It is neither by stirring up expectations about the return of totalitarian societies nor by adopting a complacent stand on the new applications of NSMT that the Québec government will successfully take the full measure of the changes currently underway as well as those which will continue to be seen in this area. An attitude that strives towards an appropriate balance between prudence and audacity, suspicion and naiveté, and that favours concerted actions among its main players, public consultation and sensitization, as well as an appropriate ethical framework is, consequently, duly required.

1. Definition from the Commission nationale de l'informatique et des libertés (CNIL – France), as stated in OFFICE PARLEMENTAIRE D'ÉVALUATION DES CHOIX SCIENTIFIQUES ET TECHNOLOGIQUES, *Les méthodes scientifiques d'identification des personnes à partir de données biométriques et les techniques de mise en œuvre*, op. cit., p. 8.

Chapter 1
The deployment of new surveillance and monitoring technologies: A phenomenon in line with Modernity[2]

Why is the deployment of new technologies in surveillance and monitoring currently expanding at such a meteoric rate? To answer this question, the context that fuels the demand for such technologies must be put in perspective. This context is characterized by a desire for greater security, which possibly echoes a broader sense of insecurity. In an attempt to gain a better understanding, the Commission begins its analysis with the notion of insecurity then moves on to a look at the increasing prevalence of risk and surveillance in society. In addition, the Commission presents an overview of the values and ethical issues that have been raised in its study of the deployment of NSMT for security purposes. This overview is then followed by a presentation of the normative framework that currently exists in this area.

Security: Defining the concept

What is security? Merely asking the question raises the concept's complex nature. In fact, not only does the term evoke a variety of meanings, particularly at the sociological level, but its very interpretation also varies among languages, views, approaches and history. Four key questions punctuate the debate on the notion of security[3]: "What is the nature of the insecurity?"; "What is the object of security?"; "Who will assume responsibility?"; and "What are the methods used to ensure security?".

Security includes two components[4]: 1) One is objective, and involves parameters that allow for an assessment of the actual level of security or absence of threats and dangers; 2) the other is subjective, and refers to how people feel about their own safety. Both of these dimensions are mutually influential.

Providing security for a territory, a country, city or home is a constant challenge which involves accurate threat assessment and the implementation of effective protection systems. Today, and especially since the events of September 11th, 2001, entirely new threat and security issues have emerged and would seem to require the implementation of equally new measures at both the technical and political levels. Although these events remind us that our societies are never completely safe, their impact has mostly been felt on the public sense of insecurity. The implementation of NSMT may be part of what can be called the dramatization of security, or a way of reassuring the public with regards to their security.

A sense of insecurity: An elusive fact

The notion of a sense of insecurity is very nebulous. As with the concept of security, it is important to draw the distinction between insecurity and the *sense* of insecurity.

2. "Modernity" is used in its philosophical sense. It refers to both the philosophical movement and the historical period where this movement was dominant. Larousse's *Le Grand Dictionnaire de la philosophie* presents the following definition: "The quality of what can be determined as modern, identifying more with an eye towards the future than with its break with the past: Modernity undergoes today tomorrow's onslaught, it senses what will be as much as it denounces what is no more. One must separate it from actuality which is limited to reporting today with no concern for prophecy."
3. Isabelle MASSON, 'Sécurité', in Alex MACLEOD, Évelyne DUFAULT and F. Guillaume DUFOUR (dir.), *Relations internationales: théories et concepts*, (Montréal: Athéna éditions, 2004), p. 216.
4. WORLD HEALTH ORGANIZATION, *Safety Promotion: Conceptual and Operational Aspects*, September 1998, p.7.

Insecurity is a "lack of security", a "situation where one is threatened, exposed to danger[5]", whereas the sense of insecurity is an emotional state which is the result of a subjective assessment of danger. This feeling varies from one person to another according to a variety of factors such as self-confidence.

In this Position statement, the Commission focuses on the *sense* of insecurity. Although security decisions on the part of public and private organizations may be motivated by real threats, actions are more often taken on the basis of the perception of such threats. In this respect, the deployment of NSMT will not systematically prevent crimes from being committed, but rather help reassure the public.

An important distinction needs to be drawn with regards to a sense of insecurity. First, we must distinguish between a concern for security, or generalized fear, "a generalized fear of crime as a societal phenomenon, often associated to favourable views on the hardening of the repressive apparatus[6]", and tangible fear, such as a fear of crime, which pertains to "a personal apprehension stated by the individual within a specific context". These two sentiments do not necessarily go hand in hand: An individual may well feel that insecurity is a serious problem without feeling a personal sense of danger, and vice-versa. In addition, these two levels of insecurity lead to different reactions, different needs, and are of different origins[7]. Thus, generalized fear takes root in ideas and attitudes maintained towards crime, criminals and justice in general, whereas tangible fear must be considered in the context of an individual's specific life situation. Overall, it can be stated that generalized fear is more pervasive than tangible fear[8].

The role of the media

The media would have us believe that crime is everywhere. The widespread media coverage of crime and extraordinary events (natural disasters, terrorist attacks, wars, etc.) generate a level of fear that is disproportionate to statistics on the subject[9]. Media coverage of certain events fuel the collective imagination and influence public apprehension towards various dangers[10]. Thus, greater concern will be directed to a serious but rare danger, such as a terrorist attack, than a more common danger pertaining to daily life, such as a car accident. Moreover, media coverage of crime statistics and news reports about criminal acts are disproportionate: "Whereas news reports on lower crime statistics barely make a ripple once a year when statistics are published, crime stories are reported daily by the media[11]"

If the influence of the media is so high, it is that the perception of danger is a key factor in the public's sense of insecurity. Thus, the media has an impact on this perception, as demonstrated by an investigation by the *ministère de la Sécurité publique*[12] and the most recent survey on victimization by Statistics Canada[13]. One only needs to look at the increasing number of specialized round-the-clock news networks and their popularity to become aware of the social importance given to the news media and their message.

Politics and fear of crime

In addition to the media, various players also feed into the public sense of insecurity, such as the political elite and interest groups[14]. An eloquent example can be found in a document prepared for the *Ministère de la Sécurité publique*:

5. 'Insécurité', in *Le Petit Robert*, ed. 1993, p. 1182.
6. Patrick PERETTI-WATEL, *Sociologie du risque*, (Paris: Armand-Colin, 2000), p. 162.
7. MINISTÈRE DE LA SÉCURITÉ PUBLIQUE DU QUÉBEC, *Partners in Crime Prevention: For a Safer Québec*, Report of the Task Force on Crime Prevention, 1993, available at <http://www.msp.gouv.qc.ca/prevention/prevention_en.asp?txtSection=publicat&txtCategorie=table_ronde>.
8. MINISTÈRE DE LA SÉCURITÉ PUBLIQUE DU QUÉBEC, op. cit.
9. David LE BRETON, *Sociologie du risque*, (Paris: Presses Universitaires de France, 1995), p. 35.
10. Ibid.
11. Olivier LAMALICE, *Public Position statements, incarceration and the American penal system: The influence of the political elite and the media* (in French), document d'appoint préparé pour le ministère de la Sécurité publique, p. 26. <http://www.msp.gouv.qc.ca./reinsertion/publicat/severite_penale/severite_penale_partie1.pdf>.
12. MINISTÈRE DE LA SÉCURITÉ PUBLIQUE DU QUÉBEC, op. cit.
13. STATISTICS CANADA, *General Social Survey on Victimization, Cycle 18: An Overview of Findings*, (Ottawa, Canada, 2004) p. 7. Available at <http://dsp-psd.pwgsc.gc.ca/Collection/Statcan/85-565-X/85-565-XIE.html>.
14. Corey ROBIN, *Fear. The History of a Political Idea*, (New York: Oxford University Press, 2004), p. 16.

> *The often-erroneous public perception of crime in the United States is influenced by increased media coverage of criminal acts, by widespread ghetto violence and the political capital generated by this type of coverage. As the number of news reports pertaining to crime doubled between 1992 and 1993 and overall crime rates have been dropping since 1980, President Clinton introduced strict crime legislation to Congress in 1993, taking advantage of the current favourable political climate*[15].

Fear of crime plays an undeniable political role and may be considered as an object of governance[16]. First, strategies are put in place to reassure the public by attempting to reduce or contain its fear of crime. This fear can also be used, however, for the purpose of getting individuals to adopt behaviours and life habits that reduce the likelihood of their becoming a crime victim. In short, in order to motivate individuals to remain prudent, a middle ground must be struck between reducing fear of crime that frightens and paralyses, and the use of fear as a reminder of crime-related dangers.

This reminder of the awareness of crime-related dangers lies in the wake of a general philosophy of fear. From Alexis de Tocqueville to Hanna Arendt, several Western philosophers consider fear as an instrument which can galvanize action and contribute to the preservation of hard-won liberties[17]. According to this school of thought, a fear of the return of Gulags and concentration camps would lead societies to do anything to avoid seeing these atrocities repeated. With regards to the environment, philosopher Hans Jonas has renewed this concept of fear as a guide to prudent and responsible action through the heuristic concept of fear[18]. Jonas claims that developments in science and technology make it possible, for the first time in history, for humanity to self-destruct. Past and anticipated future disasters can thus serve to guide humanity in its search for responsible actions that do not compromise current and future human living conditions.

The scope of the sense of insecurity: What are we afraid of?

It is important to know if the facts support the existence of a sense of insecurity, and if so, to identify the objects of this fear. The Commission has therefore analyzed several studies and investigations into the matter.

The sense of insecurity is difficult to quantify, and the questions posed in these studies and investigations are often rather vague. In most cases, these questions seek to find out if people feel safe at home, of if they are afraid of walking in the streets alone at night. In this area, studies are unequivocal. According to a survey by Léger Marketing[19] in January 2003, almost all Canadians feel safe at home (97%). Moreover, 84% of Canadians are not afraid to go out alone during the evening or at night. A survey[20] on the sense of security of Montrealers is also revealing: 90% of those surveyed feel safe in the Metropolitan area, and 73% feel that public transportation is safe. A 2007 survey[21] revealed that, according to 70% of respondents, Montreal is a safe city. Finally, the general social investigation conducted by Statistics Canada in 2004 reveals that Canadians feel more and more safe, which is contrary to the trend reported fifteen years ago:

> *Satisfaction with personal safety has continued to grow since 1993 and now stands at 94% of the Canadian population aged 15 years and over. The figure remains high but is somewhat lower when Canadians are asked to rate their feelings of safety in a variety of situations. For instance, four out of five people (80%) indicated that they were not at all worried when home alone at night. (…)*
>
> *Results from the 2004 GSS reveal that almost six in ten Canadians (58%) believed that their neighbourhood crime rate has remained unchanged over the past five years. Another 30% of the population were of the opinion that crime had worsened in their community, while 6% expressed the belief that crime had dropped. In general,*

15. Olivier LAMALICE, op. cit., p. 2.
16. Murray LEE, 'Governing "Fear of Crime"', in *Hard Lessons*, Richard HIL and Gordon TAIT (dir.), (Ashgate: Hants, 2004), p. 35.
17. Corey ROBIN, op. cit., pp. 9-10.
18. See Hans JONAS, *Le principe responsabilité: une éthique pour la civilisation technologique*, (Paris: Éditions du Cerf, 1990).
19. LÉGER MARKETING, *Feelings of Safety Among Canadians*, January 2003.
20. LÉGER MARKETING, *Étude sur le sentiment de sécurité des Montréalais*, March 2004.
21. LÉGER MARKETING, *Montréal une ville sécuritaire, attrayante mais malpropre*, February 2007.

> *opinions have improved since 1993, when Canadians were more likely to say that crime in their neighbourhood was on the rise (46%) than they were to say that crime was unchanged from five years earlier (43%). (…)*
>
> *In 2004, the overwhelming majority of Canadians were satisfied with their safety from being a victim and this proportion is growing. Fully, 94% of Canadians indicated that they were somewhat or very satisfied with their safety from crime, up from 91% in 1999 and 86% in 1993*[22].

Several surveys have been conducted regarding the threat of terrorism. This threat often appears more spectacular than traditional crime. As terrorists aim to create a climate of fear and insecurity, their methods, while not always new, seek to surprise[23]. Consequently, an individual may feel safe from the dangers associated with "traditional" crime, but not feel safe from a terrorist attack, even though the likelihood of becoming a victim of crime is much higher than being a victim of a terrorist attack, at least in Canada.

This said, does the population of Québec and Canada feel threatened by terrorism? What do opinion polls and investigations published in Canada reveal on this subject? Since the events of September 11th, the Canadian firm Compas has conducted an annual survey among the country's business community[24]. This survey systematically considers the question of feelings of safety among respondents. In November 2001, when asked "according to you, what is the probability that a terrorist attack of the magnitude of the World Trade Center attacks on September 11th, 2001 will occur in Canada over the next 12 months?", business people estimated this probability at 20%. This probability decreased to 12% and 15% in 2002 and 2003. Since then, on two occasions, each time following other terrorist attacks, this probability increased. In August 2004 (attacks in Madrid in March of the same year), the probability climbed to 23% and in July 2005 (attack in London the same month), the figures reached 24%. The problem with these types of questions is that they are somewhat incomplete. The answer reflects people's estimate of the probability that a terrorist attack will occur, as opposed to whether or not they feel safe knowing such an event could occur.

Interestingly, when asked about the main reason Canada could become an eventual target, 45% of respondents pointed to what they considered mediocre security and border control in Canada. One 2002 survey conducted by Léger Marketing[25] indicates that the vast majority of Canadians (94%) felt that Canada is a safe country. Nevertheless, 82% of Canadians wanted the government to spend as much or more on the country's security. Moreover, 56% of Canadians felt that a terrorist network could easily slip by Canadian security systems. In a February 2003 EKOS poll, respondents felt that the best long-term solution to protect Canada against terrorism was an increase in spending on security and information services.

Another poll, this time conducted by Strategic Counsel[26] in August 2005, revealed that 62% of respondents believed that a terrorist attack would occur in Canada in the coming years. In addition, only 25% of these believed that Canada was adequately prepared to deal with a terrorist attack. One year later, the same poll reported slightly different results[27]. Whereas 71% of respondents felt a terrorist attack would be perpetrated in Canada in coming years, 37% (up from 25%) felt that Canada was ready to manage the terrorist threat. Notably, 56% of these respondents felt the opposite. When questioned about the imminence of a terrorist attack, the proportion of respondents who felt Canada would be the target of terrorist attacks in the short-term dropped to 37%[28].

22. STATISTICS CANADA, op. cit., pp. 5 and 7.
23. For a definition on terrorism, see the Commission's Study Document *L'utilisation des données biométriques à des fins de sécurité: questionnement sur les enjeux éthiques*, (Sainte-Foy: 2005), pp. 16-17.
24. COMPAS, *Terror after London*, BDO Dunwoody/Chamber Weekly CEO/Business Leader Poll by Compas in the *Financial Post*, 18 July 2005, p. 5.
25. LÉGER MARKETING, *Safety in Canada According to Canadians*, Report, 2002.
26. Campbell CLARK, 'Canadians Want Strict Security: Poll', *GlobeandMail.com*, 11 August 2005, <http://www.theglobeandmail.com/servlet/story/RTGAM.20050811.wxsecurity11/BNStory/National/>
27. STRATEGIC COUNSEL, *Public Perceptions of Immigration and Terrorism*, 9 June 2006.
28. LÉGER MARKETING, *Are Other Terrorist Attacks Imminent? September 11 from the Point of View of Canadians: 5 Years Later – Part 1*, August 2006.

Surveys further reveal that Canadians do not seem particularly concerned by the threat weighing on their rights by measures to fight terrorism[29]. When asked, "Has the debate on the war on terrorism been overly geared towards measures to fight terrorism or the protection of civil liberties?" 13% of respondents stated that too much emphasis had been placed on measures to fight terrorism, and 26% felt the debate leaned too much towards the question of civil liberties. Finally, 46% of those surveyed were of the opinion that the debate had reached a proper balance between these two issues. In the United States, in a poll conducted in 2006, 68% of Americans believed they would have to give up some individual freedoms in order to secure the country against terrorism. The sense of insecurity among Americans has recently been investigated through a major survey[30]. Slightly less than one third of respondents believed their fellow countrymen felt safe with regards to a terrorist attack, while 57% were worried, and 10% felt that Americans were in danger. When asked about their personal sense of security, a little over half felt safe, 40% were worried, and only 6% felt they were in danger. In the light of these results, it would appear that Americans overestimate their countrymen's insecurity.

On the basis of these surveys, the Commission concludes that a rise in the fear of crime would be at odds with crime statistics, at least in Canada. Crime has in fact been on the decrease since the 1990's. According to Statistics Canada, the overall crime rate decreased by 3%[31] in 2006 (reaching the lowest crime rate in 25 years), following a 5% decrease in 2005[32]. This statistic obviously obscures certain facts. First of all, the number of violent crimes, which only represent 12% of all crimes committed in Canada, continues an overall downward trend that began in the mid-1990s[33]. In addition, the overall drop in the crime rate is largely attributable to a significant drop in the number of non-violent crimes, that is, crimes against property and other Criminal Code infractions[34]. Statistical reports on crime rates, particularly with regards to crimes pertaining to information technology, must be carefully interpreted. This more recent type of crime (which includes identity theft, for example) is not systematically reported by police departments, which makes it difficult to accurately assess the situation.

A society driven by insecurity, willingly or not, is more likely to constantly seek information to assess and manage risks and dangers that lie in wait. The focus is then directed to the social distribution of dangers as opposed to benefits: The goal is not to equitably share what is good among social actors, but rather to determine how to ensure that what is bad touches no one[35]. There is a negative logic at play in what German sociologist Ulrich Beck, in his seminal work on the subject, has termed the "risk society".

The place of risk in society

The obsession for risks inherent to life is relatively new and the hypotheses put forth in attempting to explain its causes are subject to debate. There is general agreement that scientific and technological developments present humanity with tremendous possibilities, including the means to destroy the very conditions under which life is possible.

What is risk?

The notion of risk is quite widespread and its meaning has taken on a connotation that reflects concerns emanating from the modern era. In fact, several specialists on the subject draw attention to an obsession to eliminate risk as an illustration of the evolution of mentalities since the last century. François Ewald, for example, believes that a universalization of the notion of risk characterizes our century and modernity in general. In addition, this author draws a distinction between meanings of the term "risk" as it is commonly used and how it is used in the insurance business, for example. In the first instance, risk is "taken as a synonym of danger, peril, an unfortunate event that can happen to someone, it designates an objective threat[36]",

29. STRATEGIC COUNSEL, *Immigration, Terrorism and National Security*, 7 August 2005.
30. New York Times-CBS News Survey, 17-21 August 2006.
31. STATISTICS CANADA, 'Crime Statistics in Canada, 2006', *Juristat*, 27.5, (July 2007), p. 2.
32. STATISTICS CANADA, 'Crime Statistics in Canada, 2005', *Juristat*, 26.4, (July 2006), p. 4.
33. Ibid., p. 5.
34. Ibid., p. 8.
35. Richard V. ERICSON and Kevin D. HAGGERTY, *Policing the Risk Society*, (Toronto: University of Toronto Press, 1997), p. 6.
36. François EWALD, *L'État providence*, (Paris: Bernard Grasset, 1986), p. 173.

whereas in the second instance, risk designates "a specific method of treatment of certain events that can happen to a group of individuals, or more exactly to values or capital owned or represented by a collective of individuals, that is to say, by a population[37]". In other words, the notion of risk is "a way to represent events, to objectify them […][38]".

In light of this interpretation, it is easy to understand why the notion of risk touches upon all areas of human activity. Moreover, as risk tends towards universalization, it also seeks sustainability. In fact, risk can be seen as an "unsurpassable horizon of the human condition[39]". Despite information campaigns, the promulgation of laws, the efforts of experts and other actions, unfortunate events continue to occur.

In general, Western societies are ambivalent with regards to risk. Individuals collectively agree to reduce risks in ways that could possibly affect entire groups. The state then reflects these agreements by developing action plans, policies and laws that aim to protect citizens and their health, or the environment. At the level of the individual, however, one does not have to look very far to see how some people are attracted to risk. The difference here being that in most cases, the risks only involve the person taking them (which is not to say that in so doing, this person becomes exposed to unfortunate consequences that could be harmful to his surroundings, such as the case of a compulsive gambler who loses everything). These risks are multiple and varied: Extreme sports, risky sexual practices, thrill seeking, gambling, drug abuse, etc. A parallel can be drawn with new surveillance and monitoring technologies. On one hand, Western societies have collectively implemented mechanisms to protect privacy and confidentiality of personal information. This is an attempt to limit the risks involved in the circulation of this type of information in private and public areas. Individual credit and debit card users, members of rewards programs and individuals who use the Internet to conduct transactions, however, take personal risks by divulging personal information in a manner that is not always secure.

The link between security and risk is illustrated by anthropologist David Le Breton as he draws attention to the shift in meaning of risk "from a reference to a probability to that of a threat or danger being a symptom of a society haunted by security and concerned with the prevention of the various forms of obstructions and misfortunes that affect the human condition[40]." Modern Western societies, having become obsessed with eliminating risk, are commonly referred to as risk societies.

Characteristics of a "risk society"

In accordance with the object of this chapter, which is to provide a contextual backdrop for the deployment of NSMT, the risk society will be addressed solely in reference to its essential characteristics[41] and as they relate to the purpose of this Position statement.

This focus is all the more necessary since German sociologist Ulrich Beck has forged this concept and developed a substantial body of work on the subject in another context: Awareness of the negative effects of modern industrialization, particularly on the environment and human health. For the purposes of this Position statement, however, this context will be excluded in favour of the spirit of the risk society and the measures implemented by such a society to manage the distribution of dangers. NSMT figure among these measures.

The risk society represents a shift in the history of mentalities. Pre-industrial society is characterized by an authoritarian and dogmatic concept of science, which was given almost boundless confidence (with an optimism that is most glaringly illustrated in the idea of progress), with a strong emphasis on production and the sharing of wealth, and relatively rigid social and family roles. The risk society breaks away from this "not by any external influence, based on a new social and political model, but on a further extension of its own principles[42]". The risk society is not only aware of the fallibility of science, but has also reached a point where

37. Ibid.
38. Patrick PERETTI-WATEL, op. cit., p. 48.
39. David LE BRETON, op. cit., pp. 25-26.
40. David LE BRETON, op. cit., p. 23.
41. Most characteristics are taken from Richard V. ERICSON and Kevin D. HAGGERTY, op. cit., p. 85-91.
42. Luc FERRY, 'La nouvelle société du risque', in *Liberté, risque & responsabilité: nouveaux repères à l'heure de la mondialisation et du terrorisme international*, (Paris: Institut français des relations internationales, 2001), p. 20.

it is no longer only nature which generates risks that merely need to be controlled, but scientific research itself as well. Furthermore, production and the sharing of wealth increasingly tend to shift towards the production and sharing of risks that result from their initial efforts. Finally, traditional social roles are called into question, as illustrated by the women's liberation movement[43].

In a risk society, uncertainty linked to threats and dangers must be reduced to the point where individuals feel confident enough for action. The notion of the risk society should be clarified: This is not a society where risks are necessarily greater, omnipresent or established, but a society that is more sensitive to all types of risks[44]. In fact, the following questions illustrate the characteristics of the risk society: "How can the risks and hazards systematically produced as part of modernization be prevented, minimized, dramatized, or channelled? Where they do finally see the light of day in the shape of 'latent side effects', how can they be limited and distributed away so that they neither hamper the modernization process nor exceed the limits of that which is 'tolerable' – ecologically, medically, psychologically and socially?[45]"

As the concept of risk is future-oriented, risk assessment assumes a projection into the future. It is possible to consider events that may occur in the future by conducting an assessment of conditions in the present:

> *The center of risk consciousness lies not in the present, but in the future. In the risk society, the past loses the power to determine the present. Its place is taken by the future, thus, something non-existent, invented, fictive as the 'cause' of current experience and action. We become active today in order to prevent, alleviate or take precautions against the problems and crises of tomorrow and the day after tomorrow – or not to do so*[46].

The risk society is narrowly connected to the development of science and technology. There are multiple complex links between risks and the development of science and technology. Two parallel phenomena are at play: On one hand the more scientific and technological knowledge grows, the more light it sheds on events previously considered as fate or destiny. From that point forward, these events are labelled as risks that could and should be eradicated. On the other hand, the development of science and technology creates new risks. Beck offers another illustration of the relationship between risk society and the development of science and technology in this statement: "The scientific concern with the risks of industrial development in fact relies on social expectations and value judgments, just as the social discussion and perception of risks depend on scientific arguments[47]". This leads to a consideration of another characteristic of the risk society.

In the risk society, consideration of risk extends beyond the domain of science. As they become involved in measuring risk, scientists are not alone to claim authority in this area. A variety of social actors, according to their perception of a specific risk, take part in the discussion as a counterweight to the scientific assessment of risks. Thus, the scientific assessment (probabilistic calculation) may differ significantly from the perception of this same risk by a group of citizens, for example.

Several psychosocial factors influence the perception of risk, such as[48]:

- **Familiarity**: Activities involving less familiar risks.
- **Scientific uncertainty**: Risks that are less known to the scientific community.
- **Involuntary exposure**: Risks to which one is exposed involuntarily.
- **Potential for disaster**: Situations involving a potential major accident or disaster.
- **Reversibility**: Activities which cause irreversible effects.
- **Effects on future generations**: Activities that involve risks for future generations.

43. Ibid., p. 22.
44. Ulrich BECK, *Risk Society: Towards a New Modernity*, Sage, 1992 p. 56.
45. Ibid., p. 19.
46. Ibid., p. 34.
47. Ibid., p. 30.
48. Adapted from Vincent T. COVELLO (1985) in BUREAU D'AUDIENCES PUBLIQUES SUR L'ENVIRONNEMENT, *Le projet de la Régie intermunicipale de gestion des déchets sur l'île de Montréal*, rapport d'enquête et d'audience publique, 1993, p. 140.

- **Equity**: Activities that involve risks that are inequitably distributed among the population.
- **Media coverage**: Risks that draw media attention.
- **Control**: Risks that individuals feel are out of their control.

The rationale behind the risk society contains an "implicit ethic". A discussion of risk cannot be considered without an implicit ethic of the risk society, or be devoid of ethical, social, cultural, economic and political leanings. The following summarizes Beck's concept of an implicit ethic of the risk society.

Implicit Ethic of the Risk Society

Risks experienced presume a normative horizon of lost security and broken trust. Hence, even where they approach us silently, clad in numbers and formulas, risks remain fundamentally localized, mathematical condensations of wounded images of a life worth living. The ideas must in turn be believed, that is, they cannot be experienced as such. In this sense, risks are objectified negative images of utopias, in which the human, or what is left of it, is preserved and revived in the modernization process. Despite all its unrecognizability, this normative horizon, in which the riskiness of the risk first becomes tangible, cannot ultimately be removed by mathematics or experiments. Behind all the objectifications, sooner or later the question of acceptance arises and with it anew the old question: how do we wish to live? What is the human quality of humankind, the natural quality of nature which is to be preserved? The spreading talk of 'catastrophe' is in this sense an objectivized, pointed, radicalized expression that this development is not wanted[49].

The risk society is directly concerned by security[50]. Governments spend much of their time and resources to ensure public safety: Food safety, civil security, national security, public security, road security, sanitary security, etc. This swing towards security stimulates an insatiable demand for better knowledge of risks. Thus, as the search for information on risk progresses, threats are more closely examined and considered as to their likelihood of occurrence and new areas of insecurity are brought to light[51]. Beck adds that "[t]he promise of security grows with the risks and destruction and must be reaffirmed over and over again to an alert and critical public through cosmetic or real interventions in the techno-economic development[52]".

In matters of national and public security, obtaining as much information as possible allows for the creation of profiles (the typical sexual offender, for example), to identify areas where crimes or terrorist attacks are more likely to occur, categories of individuals who should be placed under closer surveillance and to help the work of police officials in the field, to mention a few examples. Thus, probabilistic calculations by risk assessment experts can be used to effectively direct resources where they are needed[53]. Consequently, information gathering is absolutely vital to the risk society. This information is obtained by surveillance, among other means.

Towards a surveillance society?

In order to function properly, the risk society needs information and ways to collect it. New surveillance and monitoring technologies figure among these means of collecting information. They are precious tools that make it possible to map out risks and to evaluate the nature and quantity of resources that should be allocated to various areas of human activity.

Recently, and especially since the terrorist attacks of September 11th, 2001, a change in direction can be observed in the methods used to gather information. Surveillance is no longer restricted to what are considered "risk" segments of the population. The general public is now placed under surveillance in order to target actions against individuals considered at risk, or who present a risk to others[54]. This leads some to claim that

49. Ulrich BECK, op. cit., p. 28.
50. For a more in-depth analysis of the concept of security, see the study document of the COMMISSION DE L'ÉTHIQUE DE LA SCIENCE ET DE LA TECHNOLOGIE, *L'utilisation des données biométriques à des fins de sécurité: questionnement sur les enjeux éthiques*, (Sainte-Foy, 2005), p. 1-3.
51. Richard V. ERICSON and Kevin D. HAGGERTY, op. cit., p. 85.
52. Ulrich BECK, op. cit., p. 20.
53. SURVEILLANCE STUDIES NETWORK, *A Report on the Surveillance Society*, United Kingdom, September 2006, p. 7, available at <http://www.ico.gov.uk/upload/documents/library/data_protection/practical_application/surveillance_society_full_report_2006.pdf>.
54. Ibid., p. 12.

anticipation of a surveillance society of the future is pointless: We are already in a surveillance society[55].

Surveillance, however, is not a new phenomenon, and it did not await the advent of risk societies or advanced technology to emerge. Surveillance has been an integral part of human civilization since time immemorial, as even socialization itself would be unthinkable without adult supervision. Children learn to interact with others under the supervision of adults who watch over them. At another level, surveillance can also be considered a central mechanism through which the modern state achieves its administrative duties pertaining to health, welfare, education and public security[56].

What is surveillance?

There are many definitions of surveillance; some are all-encompassing, others clearly illustrate the complex nature of this phenomenon. A general definition, which applies equally to security, could be formulated as follows: Surveillance is "any collection and processing of personal data, whether identifiable or not, for the purposes of influencing or managing those data have been garnered[57]."

Another, more substantial definition was also considered. In this definition, surveillance involves one or more of the following activities:

- "the collection and storage of information (presumed to be useful) about people of objects;
- the supervision of the activities of people or objects through the issuing of instructions or the physical design of the natural and built environments […];
- the application of information gathering activities to the business of monitoring the behaviour of those under surveillance, and in the case of subject persons, their compliance with instructions.[58]"

Finally, one last definition, which appears to go much further into the description of certain characteristics of surveillance, is worthy of mention: When purposeful, routine and systematic attention is given to personal information in order to monitor, manage, influence or protect, surveillance is said to be involved. This definition is further clarified by the following factors:

- "The attention is purposeful; the watching has a point that can be justified, in terms of control, entitlement, or some other publicly agreed goal;
- Then it is routine; it happens as we all go about our daily business, it's in the weave of life;
- But surveillance is also systematic; it is planned and carried out according to a schedule that is rational, not merely random;
- Lastly it is focused; surveillance gets down to details. While some surveillance depends on aggregate data, much refers to identifiable persons, whose data is collected, stored, transmitted, retrieved, compared, mined and traded[59]."

The controlling effect of surveillance can sometimes be indirect or unintentional[60]. Moreover, many forms of surveillance are legitimate within a democratic framework, though their cumulative impact on the respect for the privacy of individuals is a source of concern[61].

Characteristics of a surveillance society

The rise of a surveillance society is a product of modernity[62], and is characterized by the importance given to the notion of efficiency. This translates into organizational practices that aim to quickly and adequately meet the needs of the public who expects the state to provide for some of these needs (health, security, welfare, education, etc.), and who is keenly aware of the latest

55. Ibid., p. 1.
56. Clive NORRIS and Gary ARMSTRONG, *The Maximum Surveillance Society: The Rise of CCTV*, (Oxford: Berg, 1999), p. 5.
57. David LYON, *Surveillance Society: Monitoring Everyday Life*, (Buckingham: Open University Press, 2001), p. 2.
58. Christopher DANDEKER, *Surveillance, Power and Modernity*, (New York: St. Martin's Press, 1990), p. 37.
59. SURVEILLANCE STUDIES NETWORK, op. cit., p. 4.
60. Ibid., p. 33.
61. David H. FLAHERTY, *Protecting Privacy in Surveillance Societies*, (Chapel Hill: University of North Carolina Press, 1989), p. 1.
62. Ibid., p. 1 and 2.

consumer products that better meet their requirements. Consequently, organizations constantly seek information allowing them to better know their "clientele", in order to anticipate and meet these needs. As these organizations strive for quicker and more efficient processing and control of data, they implement surveillance systems in order to collect useful information. In short, surveillance has much to do with the way in which modern societies are structured at the political and economic levels, as they promote mobility, speed, security and consumer freedom.

Given that the media often portrays the deployment of NSMT as part of the development of a more authoritarian (if not totalitarian) society, its justification is more often presented through a rationale of citizen protection[63]. This said, such a deployment, the way it is implemented and its consequences are cause for concern.

Another characteristic of the surveillance society is that it is narrowly linked to technology. This does not mean that one causes the other. Obviously, humans have not waited for this technology to appear to begin watching over one another. In the past, the use of surveillance was not particularly widespread or systematic whereas it has now become routine. Surveillance is a part of daily life, and is usually implemented by agencies and organizations from remote locations, all made possible by developments in technology.

Surveillance is becoming generalized at a number of levels. First, surveillance is no longer limited to monitoring deviants and suspects. Anyone can become the object of surveillance. Gathering large amounts of information allows for more thorough profiling in every imaginable area. A striking example is the fight against terrorism. As long as surveillance efforts are focused on suspects and individuals who appear to be associated with terrorist groups, individuals who do not fit the target profile remain unnoticed. By tracking the Internet browsing habits of all citizens, for example, authorities could find suspicious Internet users by their visits to sites linked to terrorist groups, or sites describing how to build a bomb. Perhaps more importantly, by studying the Internet surfing habits of criminals and terrorists, authorities could then build a browsing profile for the "typical terrorist". The same process could be applied to perpetrators of fraud, pedophiles, etc. The principle, however, remains the same: In order to stop criminals before they commit their offence, and to provide even more comprehensive and effective prevention, as many people as possible, even an entire population would ideally be placed under surveillance.

Such an endeavour obviously requires constant and almost omnipresent surveillance. The use of surveillance could occur just about anywhere and on a continuous basis. Some maintain that from this point forward, normal, everyday activities will be subject to surveillance. In fact, it is difficult to think of a place or an activity that is free of all surveillance[64]. Moreover, the players who operate surveillance systems are quickly expanding to include not only the state, but also private businesses and citizens, who now privately use NSMT for various purposes, including security.

An entire segment of the world of literature and movies has generated a sense of fear among the general population that, if not easily dismissed, needs to be put into perspective. Surveillance is usually portrayed in such a way that leads to widespread belief in conspiracies to control populations. Proponents of this conspiracy theory can fall into two traps: The belief that surveillance is plotted by the powerful people of this world, and thinking that surveillance is the direct product of developments in science and technology[65].

It is not really the imminent rise of a "Big Brother" that concerns the Commission, but rather the emergence of a number of "Small Brothers", or a number of organizations and individuals who privately conduct surveillance activities for security purposes that is troubling. This type of surveillance, which does not necessarily follow proper guidelines and sound practices could fall completely beyond the control of the state.

The ethical framework: The issues and values at stake

The ethical framework used by the Commission in its analysis is based on two considerations: First, since the Commission has always favoured an approach based

63. Clive NORRIS and Gary ARMSTRONG, op. cit., p. 5.
64. David LYON, op. cit., p. 1.
65. SURVEILLANCE STUDIES NETWORK, op. cit., p. 2.

on values, it seems essential to begin by offering a brief summary of those involved in this Position statement; in addition, the Commission wishes to briefly define the ethical issues raised by the deployment of NSMT. These issues are given further consideration in Chapter 3.

Values

The value of autonomy is central to liberal democratic societies. It is the value which allows individuals to live their lives as they see fit within the limits of the rights and freedoms of others. In this Position statement, it is interpreted as the expression of freedom by citizens of democratic societies, particularly with regards to the sometimes-intrusive role of the state and other organizations. In short, "no one is autonomous if subjected to the will of others[66]". In practical terms, increased citizen involvement in the design, implementation and follow-up of the various guidelines surrounding the deployment of NSMT would represent greater compliance with the democratic ideal and respect for autonomy.

The desire to promote individual autonomy among liberal democracies is rendered tangible by a commitment to a whole range of other fundamental values. Although they may conflict in certain cases, it is generally recognized that they share a common origin. They are the conditions under which autonomy becomes possible, and from that point forward, democracy itself. Among this set of values, the Commission focuses on those most concerned by the deployment of NSMT: Security, freedom, privacy, transparency, justice and equality.

The values of security and freedom are probably the first to come to mind considering the object of this Position statement, and are narrowly linked to democratic life. In a general sense, modern democracies can be seen as a more or less successful balance between the powers of the state with regards to security and the rights and freedoms of citizens. In order to exercise their sovereignty, in accordance with the political doctrine that is democracy, citizens deliberately relinquish certain practices (such as taking justice into their own hands). In exchange, they expect a guarantee that other fundamental rights and freedoms (freedom of expression, of movement, right to privacy, physical integrity, etc.) will be respected. The state thus becomes an "arbiter and defender of the citizen". Its coercive powers allow for each individual to enjoy certain freedoms and to claim certain rights without fear of being prevented from doing so by any other individual. For example, if an individual wishes to vote for particular candidate, it is the state that implements measures by which this wish can be expressed without fear of intimidation and reprisal from opponents.

Privacy is a value that is also closely related to the deployment of NSMT. Although privacy is now considered a fundamental right, it has not always been so. Throughout history, the boundary between the private and public realm has fluctuated. Some consider the current, modern era to be characterized by an increase in individualism, by which individuals withdraw into a larger and larger private realm, to the detriment of their participation in public life[67]. One must realize that this analysis loses sight of a significant ongoing battle between the state and its citizens: The increasing pressure from the state to further tighten surveillance of its citizens is met by a corresponding increase in the public's determination to guard against incursions into their private lives.

Historically, the development of the concept of privacy is related to the right to be left alone and the right to intimacy[68]. The growing value of the right to privacy is also linked to the development of individualism, through various dimensions including modern philosophical thought, socio-historic events such as the changes in dwellings in the Middle Ages (that allowed individuals to become isolated in separate rooms), and the rise of the middle class (with the financial means to build homes in such a manner as to respect the intimacy of family members). In information societies, privacy is focused less on individual protection of intimacy and personal information, but rather on "the right to control the use by others of information that concerns me[69]".

66. Laurence THOMAS, 'Autonomie de la personne', in Monique CANTO-SPERBER (dir.), *Dictionnaire d'éthique et de philosophie morale*, (Paris: Presses Universitaires de France, 2001 [1996]), p. 121.
67. For a list of authors from this school of thought, see Elia ZUREIK, Lynda HARLING STALKER and Emily SMITH, *Background Paper for the Globalization of Personal Data Project: International Survey on Privacy and Surveillance*, (Kingston: Queen's University, 2006), pp. 3-4.
68. Stefano RODOTÀ, 'Privée (Protection de la vie)', in Gilbert HOTTOIS and Jean-Noël MISSA (dir.), *Nouvelle encyclopédie de bioéthique*, (Brussels: De Boeck Université, 2001), p. 665.
69. Ibid., p. 666.

Privacy remains a difficult concept to define, as it is subject to interpretation. Rather than attempting to seek a singular precise definition, the Commission has brought together some general characteristic concepts for which there is consensus. Thus, privacy can refer to the right to be left alone, limited access to self, secrecy, the control of personal information, personhood and intimacy[70]. In addition privacy can be divided into four general concepts:

- "Information privacy, which involves the establishment of rules governing the collection and handling of personal data;
- Bodily privacy, which concerns the protection of people's physical selves against invasive procedures such as genetic tests, drug testing and cavity searches;
- Privacy of communications, which covers the security and privacy of mail, telephones, e-mail and other forms of communication; and
- Territorial privacy, which concerns setting the limits on intrusion into the domestic and other environments such as the workplace or public space. This includes searches, video surveillance and ID checks[71]".

Transparency is a democratic value which is essential to public governance; it is a show of a non-paternalistic approach that invites responsible action on the part of the various social actors[72]. In addition, based on statements from a previous Position statement, the Commission restates the importance of this value which is reflected in its desire to see that NSMT deployment not be conducted in the shadows, but in partnership with the various concerned actors and citizens who are properly informed with regards to the main issues involved.

The Commission also wishes to invoke the values of justice and equality, particularly with regards to the processing of personal information. The use of techniques such as profiling or the targeting of certain categories of individuals in order to increase surveillance effectiveness can increase the risk of discrimination and stigmatization. It is therefore essential that citizens placed under surveillance be treated in accordance with the values of justice and equality in order to avoid potentially causing irreparable harm.

Ethical issues

The Commission does not pretend to cover the entire body of ethical issues raised by this practice. Nevertheless, the following were considered to be central to its mandate.

- Assessment of the relevance, effectiveness and reliability of NSMT

In order to legitimately be deployed, NSMT must be relevant, effective and reliable. To be relevant, NSMT must be determined as the best method of achieving a given security objective. In order for NSMT to be effective, they must produce results which match initial goals. To do this, NSMT would have to reach higher performance levels so as to avoid causing harm to innocent people. Though technical, these questions require solutions. Assessment mechanisms and their results must be made readily available to the public and easy to understand. Here, the value of transparency is of utmost importance. Furthermore, NSMT must be reliable, that is to say, their operation must not create more problems than solutions. The deployment of technology perceived as reliable that would contribute to promoting a false sense of security among the public would be unacceptable.

- Proportionality of response to insecurity

An insatiable demand for security on the part of the public and technology specialists could lead to a deployment of NSMT that is disproportionate to the actual risks involved. The use of NSMT must seek to achieve a level of security deemed acceptable without going overboard. A balance must therefore be struck among the various players involved and the general public in order to come to a consensus on the matter.

70. Elia ZUREIK, Lynda HARLING STALKER and Emily SMITH, op. cit., pp. 1-2.
71. PRIVACY INTERNATIONAL, *Overview of Privacy*, 29 October 2006. <http://www.privacyinternational.org/article.shtml?cmd[347]=x-347-543673&als[theme]=Privacy%20and%20Human%20Rights>.
72. COMMISSION DE L'ÉTHIQUE DE LA SCIENCE ET DE LA TECHNOLOGIE, *Pour une gestion éthique des OGM*, (Sainte-Foy: 2003), p. 63.

- Social acceptability

The true measure of social acceptability of NSMT deployment is difficult to determine. Better knowledge of public perceptions and opinions in this area would certainly help provide further insight into the issue. It is important that more be known about the views of citizens with regards to NSMT. A voice must be given to those who will be placed under surveillance in order to ensure that deployment be both acceptable to, and accepted by society.

- Consent

Consent, always an important issue, involves a number of challenges. This also holds true for consent with regards to NSMT. Due to their very nature, it is sometimes difficult, even impossible to obtain individual free and clear consent on the part of those under surveillance. In fact, individual free and clear consent is simply not a concept that can be applied to NSMT. Biometric data can be collected without a person's knowledge, surveillance cameras can capture images from a downtown street without the consent of passers by, and subcutaneous RFID implants could be impossible to refuse by certain categories of people. Various legal provisions already guide the collection and distribution of personal data collected by NSMT. Some of these provisions, however, have limitations.

- Respect for the end purpose

Respect for the end purpose to which NSMT are deployed and allowing any or all other possible uses are a source of tension. On one hand, respect for the stated end purpose is an important principle which aims to prevent function creep and certain forms of abuse and excess. On the other hand, exploitation of all other possible uses of NSMT (including ends to which individuals have not given their consent) would probably allow for increased security. But are the benefits touted by the deployment of NSMT in accordance with the respect of fundamental democratic values?

- Protection of personal information

Easily considered a major issue, the protection of personal information inevitably relates to the values of privacy and security. This issue, whether considered in the context of biometric data, video surveillance, or radio frequency identification, is complex enough to be treated separately. The Commission recalls the promises and risks associated with the deployment of NSMT, which brings to light the potential for both the management of risks and invasion of privacy.

Private and public spaces: A tenuous boundary

The boundary between public and private spaces is increasingly permeable. This observation is ethically significant since the importance of privacy is increasingly subject to debate, if not altogether called into question.

The importance and function of private and public spaces have greatly evolved through the ages, just as the boundaries that separate them. In the past, the rise of Christianity, and later, the middle class and capitalism have deeply changed the definitions and concept of private and public spaces. These notions, however, have always been interdependent[73].

Today's consumer society and the information and communications technology revolution have contributed significantly to reshaping the concept of privacy, and in so doing, blurred the boundaries that define private and public space.. For example, organizations from the public and private sectors exchange information, have shared interests, and an increasing number of government mandates are successfully carried out through joint efforts with the public and private sectors, as well as non-governmental organizations[74].

The wavering permeability of this boundary can be further illustrated in how easily data previously considered as strictly private now circulates freely through computer systems at both the public (access to government programs) and private (retail business client files) levels[75]. Although this information can always be considered personal, its circulation outside the private realm is now almost a daily occurrence.

73. David LYON, *The Electronic Eye*, (Minneapolis: University of Minnesota Press, 1994), pp. 183-184.
74. SURVEILLANCE STUDIES NETWORK, op. cit., p. 36.
75. David LYON, *Surveillance Society: Monitoring Everyday Life*, (Buckingham: Open University Press, 2001), p. 17.

Finally, it must be mentioned that the advent of the Internet has drastically changed the connection between individuals and their private lives. It is now possible, for example, to post photo albums or videos online, to expose one's life on blogs, or participate in other activities that reveal many aspects of one's private life. Are these individuals more exhibitionistic or voyeuristic than before? Are we witnessing the dawn of a redefinition of privacy? The Commission has certainly been mindful of these questions throughout its deliberations.

Normative instruments currently in place

Since the concept of personal information is a recurring theme in the discussion of NSMT, and that the use of certain technologies (particularly radio frequency identification) raises legal issues pertaining to their meaning, it appears essential to consider current relevant legal definitions. In addition, the main laws that govern the deployment of NSMT and the collection, use, sharing and retention of personal information will be presented.

Legal definitions of personal information

In Québec, the Act respecting the protection of personal information in the private sector defines personal information as "any information which relates to a physical person and allows that person to be identified[76]". Using essentially the same words, the Act respecting access to documents held by public bodies and the protection of personal information offers the following definition of the term "personal information[77]": "In any document, information concerning a natural person which allows the person to be identified is personal information". It is important to note that generally speaking, personal information is confidential, unless "the person to whom the information relates consents to its disclosure[78]".

In Canada, the Privacy Act defines personal information as follows:

"personal information" means information about an identifiable individual that is recorded in any form including, without restricting the generality of the foregoing,

(a) information relating to the race, national or ethnic origin, colour, religion, age or marital status of the individual,

(b) information relating to the education or the medical, criminal or employment history of the individual or information relating to financial transactions in which the individual has been involved,

(c) any identifying number, symbol or other particular assigned to the individual,

(d) the address, fingerprints or blood type of the individual,

(e) the personal opinions or views of the individual except where they are about another individual or about a proposal for a grant, an award or a prize to be made to another individual by a government institution or a part of a government institution specified in the regulations,

(f) correspondence sent to a government institution by the individual that is implicitly or explicitly of a private or confidential nature, and replies to such correspondence that would reveal the contents of the original correspondence,

(g) the views or opinions of another individual about the individual,

(h) the views or opinions of another individual about a proposal for a grant, an award or a prize to be made to the individual by an institution or a part of an institution referred to in paragraph (e), but excluding the name of the other individual where it appears with the views or opinions of the other individual, and

(i) the name of the individual where it appears with other personal information relating to the individual or where the disclosure of the name itself would reveal information about the individual […][79].

The Personal Information Protection and Electronic Documents Act, for its part, defines personal information as "information about an identifiable individual, but does not include the name, title or business address or telephone number of an employee of an organization[80]."

76. R.S.Q., chapter P-39.1, 1993, c. 17, s. 2.
77. R.S.Q., chapter A-2.1, 1982, c. 30, s. 54; 2006, c. 22, s. 110.
78. R.S.Q., chapter A-21, 1982, c. 30, s. 53; 1985, c. 30, s. 3; 1989, c. 54, s. 150; 1990, c. 57, s. 11; 2006, c. 22, s. 29.
79. R.S., 1985, c. P-21 s. 3.
80. *Personal Information Protection and Electronic Documents* Act, R.S., 2000, c. 5, P-8.6, part 1 s. 2.

In Europe, Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data offers a very broad definition of what constitutes personal data: "any information relating to an identified or identifiable natural person ('data subject'); an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity; […][81]".

Protection of privacy and personal information in Québec[82]

In Québec, section 5 of the Charter of Human Rights and Freedoms and sections 35 to 41 of the Civil Code guarantee the right to privacy for all individuals.

Québec laws provide specific obligations that govern the collection, use, retention and sharing of personal information. These obligations are specified in the following Acts:

The Act respecting Access to Documents held by Public Bodies and the Protection of Personal Information (R.S.Q., chapter A-2.1) – This Act applies to documents kept by a public body in the exercise of its duties, whether it keeps them itself or through the agency of a third party, it also governs access to these documents.

The Act respecting the protection of personal information in the private sector (R.S.Q., chapter P-39.1) – This Act establishes the "particular rules with respect to personal information relating to other persons which a person collects, holds, uses or communicates to third persons in the course of carrying on an enterprise".

The Act to establish a legal framework for information technology (R.S.Q., chapter C-1.1) – This Act aims to ensure that:

- "the legal security of documentary communications between persons, associations, partnerships and the State, regardless of the medium used;
- the coherence of legal rules and their application to documentary communications using media based on information technology, whether electronic, magnetic, optical, wireless or other, or based on a combination of technologies;
- the functional equivalence and legal value of documents, regardless of the medium used, and the interchangeability of media and technologies;
- the linking of a person, an association, a partnership or the State with a technology-based document, by any means allowing them to be linked, such as a signature, or any means allowing them to be identified and, if need be, located, such as certification; and concerted action for the harmonization of the technical systems, norms and standards involved in communications by means of technology-based documents and interoperability between different media and information technologies.[83]"

The Private Security Act (R.S.Q., chapter S-3.5) – This Act (although only certain provisions are currently in force) applies to the following private security activities:

- "security guarding, namely, watching or protecting persons, property or premises mainly to prevent crime and maintain order;
- activities related to electronic security systems, namely, installing, maintaining and repairing, and ensuring the continuous remote monitoring of, burglar or intrusion alarm systems, video surveillance systems and access control systems, except vehicle security systems; […][84]"

Finally, Québec has the distinction of having put in place a legal framework to protect its citizens with regards to biometrics. Since 2001, the Act to establish a legal framework for information technology deals in part

81. EUROPEAN PARLIAMENT AND THE COUNCIL OF THE EUROPEAN UNION, 'Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data', *Official Journal* L 281, 23/11/1995 P. 0031 – 0050, available at <http://europa.eu.int/eur-lex/lex/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:EN:HTML>
82. The Commission would like to thank Ms Danielle Parent for her collaboration to this section's content.
83. R.S.Q., chapter C-1.1, 2001, c. 32, s. 1.
84. R.S.Q., chapter S-3.5, 2006, c. 23, s. 1.

with the concerns raised by the use of biometrics. Thus, according to section 44 of this Act, "a person's identity may not be verified or confirmed by means of a process that allows biometric characteristics or measurements to be recorded, except with the express consent of the person concerned. Where consent is obtained, only the minimum number of characteristics or measurements needed to link the person to an act and only such characteristics or measurements as may not be recorded without the person's knowledge may be recorded for identification purposes". Section 45 adds the obligation to disclose the creation of any biometric characteristic or measurement data bank to the *Commission d'accès à l'information (CAI)*. By virtue of this provision, the CAI is given various powers to, for example, suspend or forbid the implementation of a biometric data bank, and even order its destruction.

In the preparation of its study document[85], the CAI has defined nine biometric application principles based on the combined effects of the three Québec Acts. These principles, accompanied with a series of questions designed to guide any person wishing to use biometrics within their organization, are[86]:

1) Alternatives to biometrics;
2) Necessity of information collected;
3) Collection from the person concerned;
4) Consent to use of biometrics;
5) Retention and use of biometric data;
6) Use of biometric data;
7) Communication of biometric data;
8) Destruction of biometric data;
9) Rights of access and correction.

In addition to the three Acts mentioned above that govern the collection, use, retention and sharing of personal information in both the public and private sectors, Québec, through the CAI, has developed a set of regulations governing the use of video surveillance with recording in public places by public organizations[87].

At the time of its public consultation on video surveillance, the CAI had already prepared a less complete version of these regulations, and used the occasion to launch a debate on a normative framework for video surveillance. The direction favoured by most consulted was to adopt a policy framework or regulation so that "the use of video surveillance would be subject to a binding legal mechanism" and to "not leave it up to the sole judgement of public administrators to decide on whether or not to use video surveillance[88]".

With regards to radio frequency identification, no legal provisions pertaining specifically to this technology were found among the laws and regulations of Québec. It is nevertheless important to report the publication of a CAI study document[89], which to a certain extent represents the beginnings of a framework for the use of radio frequency identification.

Protection of privacy and personal information in Canada

At the federal level, section 8 of the Canadian Charter of Rights and Freedoms and part 6 of the Criminal Code recognize privacy as a fundamental right.

Federal law includes a body of legal texts that govern, in a general sense, the collection, use, retention and sharing of personal information. In fact, two Canadian laws specifically pertain to protection of personal information:

85. COMMISSION D'ACCÈS À L'INFORMATION DU QUÉBEC, *La biométrie au Québec: les enjeux*, Analytical Document, July 2002, available at <http://www.cai.gouv.qc.ca/06_documentation/01_pdf/biom_enj.pdf>.
86. COMMISSION D'ACCÈS À L'INFORMATION DU QUÉBEC, *Biometrics in Québec: Application Principles, Making an Informed Choice*, July 2002, available at <http://www.cai.gouv.qc.ca/home_00_portail/01_pdf/biometrics.pdf>.
87. See Appendix 1.
88. Michel LAPORTE, *Bilan*, Public consultation: Use of surveillance cameras by public bodies in public places, (Commission d'accès à l'information, April 2004), pp. 35-36, available at <http://www.cai.gouv.qc.ca/06_documentation/01_pdf/bilan.pdf>, [Translator's note: a summary of this report is available in English at <http://www.cai.gouv.qc.ca/06_documentation/01_pdf/summary_report.pdf>].
89. COMMISSION D'ACCÈS À L'INFORMATION DU QUÉBEC, *Radiofrequency Identification Technology (RFID): Is there Reason to Mistrust It?* , Analytical Document, May 2006, available at <http://www.cai.gouv.qc.ca/06_documentation/01_pdf/RFID_en.pdf>.

The Privacy Act (R.S., 1985, c. P-21) – "The purpose of this Act is to extend the present laws of Canada that protect the privacy of individuals with respect to personal information about themselves held by a (Federal) government institution and that provide individuals with a right of access to that information[90]."

The Personal Information Protection and Electronic Document Act (2000, c. 5) – is "An Act to support and promote electronic commerce by protecting personal information that is collected, used or disclosed in certain circumstances, by providing for the use of electronic means to communicate or record information or transactions[91]": The first two sections of the Act each have a different purpose:

- The purpose of the first 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".
- The purpose of the second part is "to provide for the use of electronic alternatives in the manner provided for in this Part where federal laws contemplate the use of paper to record or communicate information or transactions".

Although no laws specifically govern NSMT at the federal level, certain normative texts have been written regarding the matter.

For example, the Office of the Privacy Commissioner of Canada has established four criteria for determining the privacy implications of biometric technologies and other security measures[92]:

1. the measure is demonstrably necessary to meet specific needs;
2. the measure is demonstrably likely to be effective in addressing the needs underlying the proposed deployment;
3. the loss of privacy is proportional to the security benefit; and
4. it can be demonstrated there is no less privacy-invasive measure that could achieve the same results.

In addition, the Office of the Privacy Commissioner of Canada has drawn up guidelines for the police and other law enforcement officials with respect to video surveillance in public spaces[93].

Protection of privacy and personal information at the regional and international levels

Several international texts, as well as certain texts pertaining to Europe and the United States, are worthy of mention.

At the international level, the United Nation's Universal Declaration of Human Rights, which affirms the importance of the right to privacy (in section12), is particularly noteworthy. In 1980, the Organisation for Economic Co-operation and Development (OECD) also issued guidelines entitled *OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data.*

In Europe, article 8 of the European Convention on Human Rights deals specifically with individual and family privacy rights. The 1981 Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data and Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data reaffirm the importance of the right to privacy and focus on guiding the collection, use, retention and disclosure of personal information.

90. *Privacy Act*, R.S., 1985, c. P-21.
91. *Personal Information Protection and Electronic Documents Act*, R.S., 2000, c. 5, P-8.6.
92. 'Does Facial Recognition Measure Up? Canada's Passport Office Answers the Question', *IIJ@WORK*, Summer 2004, p. 21.
93. See Appendix 2.

The Directive in brief

In order to remove the obstacles to the free movement of data without diminishing the protection of personal data, Directive 95/46/EC (the data protection directive) was developed to harmonise national provisions in this field. As a result, the personal data of all citizens will have equivalent protection across the Union. The 15 Member States of the EU were required to bring their national legislation into line with the provisions of the directive by 24 October 1998.

A directive is a piece of European legislation which is addressed to Member States. Once such legislation is passed at the European level, each Member State must ensure that it is effectively applied in its legal system. […]

The data protection directive applies to 'any operation or set of operations which is performed upon personal data', called 'processing' of data. Such operations include the collection of personal data, its storage, disclosure, etc. The directive applies to data processed by automated means (e.g. a computer database of customers) and to data that are part of or intended to be part of non-automated 'filing systems' in which they are accessible according to specific criteria. (For example, the traditional paper files, such as a card file with details of clients ordered according to the alphabetic order of the names)[94].

With regards to biometrics, the International Biometric Industry Association's initiative in the development of a self-regulatory instrument is particularly noteworthy. Out of five statements, however, only one pertains to public protection, the others dealing with business ethics and sound business practices:

> *Members believe that biometric technologies should be used solely for legal, ethical, and nondiscriminatory purposes. They are therefore committed to the highest standards of systems integrity and database security in order to deter identity theft, protect personal privacy, and ensure equal rights under the law in all biometric applications.*[95]

94. EUROPEAN COMMISSION, *Data Protection in the European Union: Dialogue with Citizens and Business*, (Belgium: 2000), p.4.
95. INTERNATIONAL BIOMETRIC INDUSTRY ASSOCIATION, *IBIA Statement of Principles and Code of Ethics*, 23 October 2000. available at <http://www.ibia.org/aboutibia/ethics.asp>.

Chapter 2
New surveillance and monitoring technologies: An overview

Faced with insecurity, caused by recent terrorist attacks in particular, states have responded by implementing security procedures that involve the use of new surveillance and monitoring technologies (NSMT): Biometrics, video surveillance and radio frequency identification (RFID). All of these technologies are currently in use, but to very different degrees. With this overview, the Commission wishes to help provide a better understanding of these technologies in order to better grasp the ethical repercussions of their implementation

Biometric systems: Under the thumb?

Aside from the use of fingerprints in the legal system, and more recently, the use of hand geometry readers to control access to certain buildings, biometric technologies are not generally known among the public. These technologies nevertheless generate considerable "fascination and anxiety[96]", to quote Jennifer Stoddart, President of the *Commission d'accès à l'information (CAI)* until 2004. In the following section, the Commission offers a description of biometric systems, their purposes, applications and operation.

Some useful definitions

The term "biométrie" has various meanings in the French language[97]. Under the influence of English, and in the realm of security, the term has come to denote "techniques that allow for an individual to be identified based on one or more of that individual's biological or behavioural features[98]".

A biometric system thus becomes a technological application that "allows a person to be automatically identified, or to verify a person's eligibility to be given certain rights or services (namely access) based on the recognition of physical attributes (fingerprints, retinal patterns, hand geometry), traces (DNA, blood, odours), or behaviours (signature, gait)[99]".

Biometric information is morphologically, biologically, or behaviourally unique to one individual. Just a few years ago, technology that could be used to measure a wide range of biometric features for identification purposes was still in its infancy, notwithstanding fingerprinting technology, the oldest and most widely used. Today, no biometric feature can be excluded out of hand, and any personal feature would appear to be biometrically measurable (to varying degrees of reliability, however): Various body parts, voice, movement, odour, body heat, etc.

Information technology plays a fundamental role in processing and analyzing this information (digitization of collected "physical" data in particular), as well as the creation of interfaces with databases containing information about individuals (personal identification, financial, medical information, etc). These technologies allow biometric systems to conduct instant mass processing with a reliability rate that can only improve in coming years – not to mention their "stealthiness", as they are increasingly blended into our surroundings.

96. Jennifer STODDART, 'Surveillance Technologies under Surveillance', Speech, September 2001, available at <http://www.cai.gouv.qc.ca/05_communiques_et_discours/discours_24_09_01-en.html>.
97. Particularly, Eugène SCHREIDER, 'science des variations biologiques, des phénomènes qui s'y rattachent et des problèmes qui en découlent', article on biometrics in *Encyclopaedia Universalis*.
98. OFFICE PARLEMENTAIRE D'ÉVALUATION DES CHOIX SCIENTIFIQUES ET TECHNOLOGIQUES, *Les méthodes scientifiques d'identification des personnes à partir de données biométriques et les techniques de mise en œuvre*, op. cit., p. 7.
99. Definition by the Commission nationale de l'informatique et des libertés (CNIL – France), as stated in OFFICE PARLEMENTAIRE D'ÉVALUATION DES CHOIX SCIENTIFIQUES ET TECHNOLOGIQUES, op. cit., note 6, p. 8.

In the realm of security, it should be mentioned that biometrics are used for two main purposes: To identify a person, or to authenticate a person (or to verify a person's identity). With the development of mass applications, however – which will enable the creation of databases that could include biometric data collected from millions of people – a third use, screening, could become widespread.

With regards to identification, the question asked is: Who is this person? The purpose is to identify an individual, often in a legal context (crime victim or having left traces at the scene of a crime), using a "one to others" type search through a centralized or local database to locate information such as fingerprints.

With identity authentication or validation, the question becomes: Is this person who he or she claims to be? This involves a "one to one" type search. Here, information supplied by the individual must match information previously colligated on some type of medium (computerized or other)[100], such as in the case of access control to buildings based on readings of an individual's hand geometry, iris or fingerprints. This type of "one to one" search does not allow for tracking and profiling of individuals, in other words, individuals or groups cannot be targeted based on their biometric features. A person's identity is validated or confirmed when that person requests a service or previously authorized access.

This distinction is important, since the risk to the protection of privacy and personal information could vary according to the biometric feature involved and how it is stored (centralized database or local computer system) as well as the purposes for which it is used.

With regards to screening, the question then becomes: Where is this person? The procedure here involves comparing data from a list of individuals under surveillance (criminals, terrorists, activists, etc.) with databases, or watch lists containing biometric samples from a large population (digital photos from passports, for instance, or from surveillance cameras) in order to extract any information that may help apprehend a criminal or suspect[101].

Purposes of biometric data

Biometric systems are used towards very specific purposes[102]:

- Crime prevention (identification of criminals, terrorists, etc.);
- Prevention of document fraud;
- Increased reliability of entitlement documents;
- Access control to rooms and physical sites;
- Access control to computer equipment (hardware and software);
- Access control to digitization equipment;
- Surveillance by security staff (continuous surveillance in real time).

Current and future technologies and their method of operation

Biometric systems can be classified according to three categories of individual-specific data:

- *Morphological or physiological data*

  This category is based on the identification of permanent physical traits that are unique to an individual. Elements used in biometric identification are generally known to be stable and more resistant to the effects of stress and aging, for instance, than

100. Information, among other sources, from CITIZENSHIP AND IMMIGRATION CANADA, *Biometrics: Implications and Applications for Citizens and Immigration*, Background Paper, Forum held October 7 & 8 2003, Ottawa, Canada, p. 2.
101. INSTITUTE FOR PROSPECTIVE TECHNOLOGICAL STUDIES, *Biometrics at the Frontiers: Assessing the Impact on Society*, Technical Report Series, 2005, p. 39-40.
102. Bernard DIONNE and Èvelyne RACETTE, 'La biométrie: présentation à la Commission de l'éthique de la science et de la technologie', Mars 2004 (manuscript).
103. Bernard DIONNE and Èvelyne RACETTE, op. cit. One must stress that some surveillance systems may analyse risk behaviours without recording the information (for example, video surveillance of a parking lot and identifying potential thieves by their behaviour).

behavioural traits[104]. Other factors, however, such as the environment and certain temporary conditions (a cold, perspiration) can affect the reliability of a reading. Morphological or physiological biometrics includes recognition of fingerprints, hand geometry, face, voice, retina (vein patterns deep inside the eye), iris, and thermography.

- *Behavioural data*

  This category involves analysis of usual and repetitive human behaviour. The underlying premise here is that the behaviour of each individual represents a personal signature. Certain movements are specific to an individual and can be used to confirm his identity. Behavioural biometrics includes signature dynamics, computer keystroke dynamics, the way a person walks, etc.

- *Biological data*

  This category involves analyses of biological traces, such as genetic "fingerprints" (DNA), odour, saliva, urine, etc.

In terms of their operation, all biometric systems involve two steps and two processes:

- User information recording;
- User information monitoring.

These two processes include five essential operational steps[105]:

1) Entry of data to be analyzed – reading of an individual's physiological, behavioural or biological features using a biometric capture terminal (or biometric sensor);
2) Data processing – Converting the information into digital data;
3) Creation and storage of a "signature" file – Digital data is used to create a model or template that represents the captured biometric information, that is to say, the signature is stored on a portable medium (tag or other) or in a database and used for comparison;
4) Comparison – A monitored (with or without their knowledge) individual's biometric features are compared to the stored "signature"; User identity then positively or negatively matches the claimed or sought identity;
5) The decision – The system operator or computerized system then decides whether the user's identity matches the claimed (authentication) or sought (identification) identity.

Biometric techniques are based on the principle that it is possible to link data to an individual, due to the uniqueness of the selected biometric feature, as well as the uniqueness of the graphic representation of this feature, both being unique to one specific individual. Biometrics are based on statistical methods used to determine the probability that two individuals share the same data (generally quite low for most current biometric data except for identical twins, and none for the iris – irises from one individual are both different).

All studies emphasize the critical importance of the recording phase. The more people collaborate throughout the process, the more biometric systems are effective.

The benefits of biometric technologies

As stated by the *Commission de l'accès à l'information*:

> *Biometrics are presented to the public as a universal remedy to a variety of ills: Terrorism, fraud, identity theft and invasion of privacy to mention but a few. To employers, it is presented as a solution to control employee time management and a way to produce data used for payroll purposes. To users, it is presented as a convenient method of identification, eliminating the need for cards that can be lost or passwords that can be forgotten*[106].

104. A report by the LONDON SCHOOL OF ECONOMICS & POLITICAL SCIENCE nuances this claim by arguing that aging not only effects the biometric data itself, but also means by which they are collected (shaking, arthritis, cataracts, falling eyelid, etc.). The report also states that no scientific study has been conducted on the stability of biometric characteristics through time. See LONDON SCHOOL OF ECONOMICS & POLITICAL SCIENCE, *The Identity Project. An Assessment of the UK Identity Cards Bill & Its Implications*, Department of Information Systems, 27 June 2005, pp. 170-175.
105. Bernard DIONNE and Èvelyne RACETTE, op. cit., and COMMISSION D'ACCÈS À L'INFORMATION DU QUÉBEC, *La biométrie au Québec: les enjeux*, Analytical Document, July 2002, pp. 8-9.
106. COMMISSION D'ACCÈS À L'INFORMATION DU QUÉBEC, *La biométrie au Québec: les enjeux*, Analytical Document, July 2002, p. 23.

In his report to the French Senate, *député* Christian Cabal states that biometric systems have proven effective in the battle against electronic and document fraud (billions of dollars for credit cards on an international scale), in providing security for financial and commercial transactions, legitimate access to government services, and in deterring identity theft in all its forms[107].

Biometrics are usually presented as technologies that can help, at least in part, eradicate identity theft. Identity documents, credit cards, and entitlement documents for access to social services, for example, are precious documents that are frequently the target of fraud. Theoretically, inserting biometric data into these documents should help deter fraud, since the criminal would face a considerable challenge in having to modify the document's biometric data to match his own, or inversely, to modify the latter to match those found in the document.

This said, biometric identity theft could lead to far greater consequences than conventional identity theft. It would in fact be very difficult to prove, and restoring the connection between biometric data and its proper owner could prove to be just as complex. Québec's CAI adds that:

> *The stability of biometric measurements or characteristics used as identifiers could become a real nightmare for victims of identity theft. Even if they managed to prove their innocence, their personal identifier would forever be compromised […]. Similarly, any malevolent individual who could manage to add his biometric information to the identity of another could cause great harm and irreparable damage to the victim of such a stratagem*[108].

On the whole, proponents of biometric technologies claim that the personal features collected and analyzed by these systems can never be used for anything other that their intended purposes for the following reasons[109]:

- Uniqueness of biometric data;
- Powerful encryption mechanisms that ensure confidentiality;
- One-way processing, to ensure anonymity. This function features a recording process that does not allow images of fingers, faces, hands, genetic codes, color, etc., to be reproduced. Therefore, analysis of the signature file alone does not allow for the individual concerned to be identified (or to identify any pathology).
- Signature mechanism for reference files, to ensure their authenticity and integrity;
- Mechanisms to deter forgery.

The use of biometric data can claim the following benefits[110]:

- Improve the security of individuals (or lower victim distress);
- Effectively protect personal information;
- Effectively deter fraud, since each individual has unique physical, behavioural or biological features that can neither be lost nor stolen;
- Counter the proliferation of passwords and the need to memorize them – inasmuch as people often tend to write them down somewhere, or use easy to guess passwords and PINs (birth dates, child names, etc.);
- Counter scams – A practice whereby computer pirates masquerade as specialists, technicians or authorities in order to steal personal identifiers or passwords.

The drawbacks of biometric technologies

The drawbacks of biometric technologies mostly pertain to information systems used relative to[111]:

- The threat of unnecessary collection;
- Processing (risk of restricting individual freedoms);
- (Unauthorized) disclosure of information;
- Interconnection of databases facilitated by the use of a unique identifier (end purpose);
- Cost.

107. OFFICE PARLEMENTAIRE D'ÉVALUATION DES CHOIX SCIENTIFIQUES ET TECHNOLOGIQUES, op. cit., pp. 46-51.
108. COMMISSION D'ACCÈS À L'INFORMATION DU QUÉBEC, *La biométrie au Québec: les enjeux*, Analytical Document, July 2002.
109. Bernard DIONNE and Èvelyne RACETTE, op. cit.
110. Ibid.
111. Ibid.

With regards to the characteristics of biometrics, the main drawbacks include the following[112]:

- Information is intrinsically linked to the individual (possibility of discovering illnesses);
- Need to physically submit to a verification process (a method considered intrusive);
- Difficulty to dissociate from one's biometric features (uniqueness of the data) and difficulty in proving one's innocence when identity documents are falsified (forged biometric element) or usurped (stolen signature file);
- Biometric comparison which carries a level of uncertainty with regards to the validity of the accepted (false positive match) or rejected (false negative match) client, as opposed to conventional authentication systems that use passwords or tokens with 100% accuracy (true or false). The difficulty lies in finding an acceptable compromise between the security requirements (high rate of false rejections) and the need for a "friendlier" system (high rate of false acceptance).

The uniqueness of biometric data can be an advantage as well as a weakness. Unlike a password, electronic certificate or access card, it is difficult to modify biometric data collected to identify an individual, so once this data is stolen or usurped, the individual from whom this information was collected would have great difficulty in proving theft. Furthermore, biometric techniques can also be outplayed, even when equipped with mechanisms to prevent falsification. The more countermeasure mechanisms continue to develop, the more sophisticated falsification techniques are likely to become.

The following table offers a summary of the main criteria pertaining to various technologies that have been developed, or that are currently being developed, as reported by the *Office d'évaluation des choix scientifiques et technologiques* (France) and by the Organisation for Economic Co-operation and Development (OECD). It is important to note that this is a rapidly evolving area and that the "performance" indications presented in the table may have improved since the assessment of a particular technique was conducted. Furthermore, a number of adjustments could likely be made to the evaluations presented in this table, particularly with regards to reliability.

Finally, an American organization – the International Biometric Group – suggests the following classification for eight biometric techniques[113]:

- "Least to most intrusive techniques[114]: Voice recognition, keystroke dynamics, signature dynamics, hand geometry, facial recognition, fingerprint, iris-scan, and retinal-scan;
- Most to least reliable techniques: Iris-scan, retinal-scan, fingerprint, facial recognition, hand geometry, voice recognition, and tied for the least reliable, keystroke dynamics and signature dynamics;
- Least to most expensive techniques: Keystroke dynamics, voice recognition, signature dynamics, fingerprint, facial recognition, hand geometry, retinal-scan and iris-scan;
- Ease of use from highest to lowest: Facial recognition, signature dynamics, iris-scan, keystroke dynamics, voice recognition, fingerprint, hand geometry and retinal-scan."

112. Ibid.

113. Ibid., p. 40.

114. This refers to physiological intrusiveness and not to the intrusiveness of collecting of personal data *per se*.

Summary of Biometric Data

Biometric Measurement[115]	Robustness[116]	Uniqueness[117]	Accuracy[118]	Potential[119]	User Acceptance[120]	Cost	Applications
Fingerprints	Medium-High	High	Very High	High	Low-Medium	Very low-Medium	Traveller clearance, driver's license, justice system
Hand Geometry	Medium-High	High	High	Medium-High	Medium-High	Medium	Access control, traveller clearance,
Finger Geometry	Medium-High	N/A	Medium-High	N/A	Medium-High	Medium	Access control, amusement park tickets
Facial Recognition	Medium	High	Low	Medium	High	Medium	Casinos, traveller clearance
Iris Scanning	High	Very High	High	High-Very High	Medium-High	Very High	Prisons, access control, traveller clearance
Retinal Scanning	High	Very High	High	N/A	Low	High	Access control, traveller clearance
Dynamic Signature Verification	Low-Medium	Medium	Low	Low-Medium	Medium-High	Low	Low security applications, applications with existing 'signature'
Voice Recognition	Medium	Medium-High	Medium-High	Medium-High	High	Low	Low security applications, Telephone authentication
Body Odour Measurement	Level Unknown	Level Unknown	Low	Level Unknown	N/A	N/A	N/A
Ear Geometry	Level Unknown	Level Unknown	Low	Level Unknown	N/A.	N/A	N/A
Thermal Imagery	Level Unknown	Level Unknown	Low	Level Unknown	N/A	N/A	N/A
Keystroke Dynamics	Level Unknown	Level Unknown	Low	Level Unknown	N/A.	N/A	N/A

Sources: *OFFICE PARLEMENTAIRE D'ÉVALUATION DES CHOIX SCIENTIFIQUES ET TECHNOLOGIQUES* (France)[121] and OECD[122].

The biometrics market

According to Citizenship and Immigration Canada, biometrics industry revenues totalled 601 million dollars U.S. in 2002, and an estimated 4 billion dollars by 2007, due to growing government and business interest in this technology[123]. Estimates for 2007 are slightly lower at 3 billion dollars. An expected steady growth rate should lead to revenues totalling 7.4 billion dollars U.S. by 2012[124].

In August 2004, Industry Canada estimated around 200 businesses across Canada to be in three niche security areas: Authentication, biometrics and cyber security, a

115. Because it cannot be analysed on the spot, DNA testing has not been included in this table. Technological improvements should correct this situation in the near future. Gait recognition has also been omitted since sources used had not proceeded to its evaluation.
116. Robustness indicates the biometric element's stability over a period of time; see OFFICE PARLEMENTAIRE D'ÉVALUATION DES CHOIX SCIENTIFIQUES ET TECHNOLOGIQUES, op. cit., p. 37.
117. Uniqueness is the ability to distinguish one individual from another; see Ibid.
118. Accuracy considers error rates: false rejects and false acceptances.
119. Based on robustness, uniqueness and accuracy, the biometric potential measures the level of safety associated with the biometric element; see OFFICE PARLEMENTAIRE D'ÉVALUATION DES CHOIX SCIENTIFIQUES ET TECHNOLOGIQUES, op. cit., p. 37.
120. Data on user acceptance cost and existing applications are from the OECD, *Biometric-based Technologies*, Working Party on Information Security and Privacy, Directorate for Science, Technology and Industry, Committee for Information, Computer and Communications Policy, Paris, 28 April 2004.
121. OFFICE PARLEMENTAIRE D'ÉVALUATION DES CHOIX SCIENTIFIQUES ET TECHNOLOGIQUES, op. cit., p. 38 et 39.
122. Ibid., p. 36.
123. CITIZENSHIP AND IMMIGRATION CANADA, *Biometrics: Implications and Applications for Citizens and Immigration*, Background Paper, Forum held October 7 & 8 2003, Ottawa, Canada, p. 6.
124. INTERNATIONAL BIOMETRIC GROUP, *Biometrics Market and Industry Report 2007-2012*.

third of which are located in the greater Montréal area[125]. This market is currently in full expansion and could influence decisions regarding the use of biometric data for security purposes. Although the Commission has not conducted an exhaustive study of this question, it seems useful to consider the subject in order to gain insight into possible eventual ethical implications.

The overall market is known to be difficult to grasp[126], since it is fragmented according to the type of biometric data used as well as the systems that have been developed (large fingerprint identification systems, for instance, which represent about 25% of the international market, and small terminals or biometric sensors used to measure a variety of biometric data). At the international level this market is largely dominated by American companies and fingerprinting technology.

The industry currently has the wind in its sails due to efforts by states to modernize and harmonize legal identification instruments in the interest of collaboration as well as the intention of several governments to attribute biometric identities to their citizens. Some, however, feel that the need for standardization could become a competitive factor[127]. Standardization aims to facilitate communications and the interoperability of biometric systems (access to information or databases by different systems) and hence, data comparison, and also help avoid user dependency on proprietary systems, harmonize methods and performance assessment principles and determine which tools are required to ensure border security[128]. The issue of standardization is both political and economic. This leads to the question as to whether countries with better technology would impose their own requirements with regards to privacy and the protection of personal information.

Public interest in biometrics[129]

The two most recent attempts at gauging public interest in biometrics are a consultation conducted by Citizenship and Immigration Canada in 2002 and 2003, and a survey done by TNS/TRUSTe in 2005.

A telephone survey was conducted in Canada in November 2002 concerning the possible creation of a national identity card with biometric data. In February 2003, sixteen consultation groups made up of citizens and permanent residents voiced their opinion on the matter. In October 2003, Citizenship and Immigration Canada held a public forum on the effects and applications of biometrics on citizenship and immigration, and later published the results.

The survey revealed that the majority of Canadians were in favour of the development of an identity card that would include a biometric identifier such as fingerprints or retinal scans in order to deter the fraudulent use of identity documents (73%), passports or various access documents for government services (80%). Nevertheless, some believe this technology is at odds with the values of freedom and equality (36%) and would hinder the protection of personal information (53%).

From these consultation groups, those in favour of the implementation of a card with biometric data saw the following advantages: Increased security, better control of borders and immigration, reduction of fraudulent use of government programs, and Canadian leadership in identification technology. Opponents raised the following concerns: Cost, infringement on privacy, freedom, system management, and opposition to United States-led security programs.

A number of papers were presented to the Standing Committee on Citizenship and Immigration. They clearly state that "Canadians want assurances that the use of biometrics technology is consistent with generally accepted privacy principles and Canadian values[130]". Some fear the intrinsically intrusive nature of biometrics that can involve private information, such as state of health – iris-scan and diabetes or hypertension, fingerprints and Down's or Turner's syndrome – as well

125. See INDUSTRY CANADA, *Canadian Security Industry Hotspots*, available at <http://www.ic.gc.ca/epic/site/ict_c-g_tic.nsf/en/tk00526e.html>

126. See OFFICE PARLEMENTAIRE D'ÉVALUATION DES CHOIX SCIENTIFIQUES ET TECHNOLOGIQUES, op. cit., p. 49.

127. Ibid., p. 48.

128. Ibid., p. 52.

129. The information is from CITIZENSHIP AND IMMIGRATION CANADA, *Biometrics: Implications and Applications for Citizens and Immigration*, Background Paper, Forum held October 7 & 8 2003, Ottawa, Canada, p. 9.

130. Ibid., p. 15.

as the potential repercussions on fundamental freedoms. The creation of an "infrastructure of surveillance" is also an area of concern, and all intrusions by the state are perceived "as offensive, invasive, and antithetical to the principles of a free and open society where values are just as important as technological advancements[131]". The forum held the following objectives:

- *Explore biometrics as a powerful technology that could meet important future policy objectives;*
- *Enhance and expand the existing discussion on technical and social issues related to the use of biometrics to strengthen document integrity and identity verification;*
- *Discuss comparative advantages and disadvantages of a comprehensive "national identity card" approach versus a more incremental strategy to improve current, multiple identity documents; and*
- *Engage in a dialogue on important issues prior to any policy implementation*[132].

Selected to bring the widest possible range of opinions, positions and points of view on identity, privacy and other related questions, participants came to the conclusion that a "Made in Canada" solution to the problem of identity documentation was required with the collaboration of provinces and territories in order to develop a national policy on these issues.

For its part, the TNS/TRUSTe survey reported the following results: 85% of Canadians were in favour of incorporating biometric identifiers into Canadian passports, which mirrored the support for the inclusion of such identifiers in other documents such as driver's permits, social insurance cards and Medicare cards[133]. In addition, more than eight Canadians out of ten felt that fingerprinting is the most acceptable form of biometric identification followed by eye scans[134] (at 67%). Main concerns among Canadians include cost of implementation, and the risks of government misuse of information.

Video surveillance: An ever-watchful eye

Video surveillance involves remote monitoring of public or private areas, using cameras, most often motorized, which transfer images taken from monitoring equipment to be viewed on a screen. Unlike the other surveillance and monitoring technologies described in this Position statement, video surveillance is not really a new technology. The Commission has included this technology for consideration for two reasons: First, recent technological advances have broadened the scope of surveillance camera capabilities. In addition to miniaturization and concealment of cameras (allowing the filming of individuals without their knowledge) and image digitization (which facilitates data storage and analysis), significant developments in intelligent software designed to detect individuals who engage in deviant behaviour are particularly noteworthy. Furthermore, potential linkage with other NSMT is another reason to include video surveillance in this analysis. In fact, image digitization allows for facial recognition of filmed individuals and comparison with other previously collected biometric data.

The pervasiveness of video surveillance is difficult to determine. Signs in public places such as shopping centres and government buildings indicate the presence of surveillance cameras. It would appear that Québecers are filmed on a regular basis. The CAI, which conducted a major public consultation on video surveillance in 2003, has offered insights into the current situation. In their report, Commissioner Michel Laporte details certain observations that describe the situation in Québec:

- *Video surveillance has been used by public bodies and operated directly under their responsibility for over 28 years;*
- *The use of surveillance cameras is neither a recent phenomenon, nor is it in decline;*

131. Ibid.
132. CITIZENSHIP AND IMMIGRATION CANADA, *Biometrics: Implications and Applications for Citizens and Immigration*, Report on a Forum held October 7 & 8 2003, Ottawa, Canada, p. 2.
133. "Canadians and Americans Support Biometric Technology in Passports and Drivers' Licences: Survey", Press release, Toronto, August 2, 2005.
134. Ibid.

- *Public bodies have expressed obvious interest in increased use of video surveillance;*
- *The use of surveillance cameras in streets, parks and public spaces is the exclusive domain of a few specific cities; […]*
- *Data on organizations that can potentially become important users of video surveillance need to be better known and documented, with the objective of further contributing to debates and overall knowledge;*
- *Private sector use of video surveillance appears rather undocumented*[135].

Two conclusions can be drawn from these observations: 1) The extent of the use of surveillance cameras is not well known; 2) this use is on the increase. This probably explains why, in addition to the CAI, several authorities have recently addressed the issue including the Office of the Privacy Commissioner of Canada[136] and organizations responsible for privacy and the protection of personal information in Alberta[137], British Columbia[138], Saskatchewan[139] and Ontario[140].

Based on a CAI survey of around fifty organizations (government ministries and organizations, municipalities, schools, etc.), an estimated 5,000 cameras were in use in 2003[141]. Since these results exclude the use of surveillance cameras in the private sector, the use video surveillance can be considered a major phenomenon in Québec, but not quite as pervasive as in countries such as the U.K, the U.S. or France.

Some useful definitions

First, it is important to consider the differences in the *types* of camera surveillance, and the different types of surveillance *cameras*. The former primarily deals with the way in which cameras are used, whereas the latter focuses on their operational features. For example, it would be possible to set up secret surveillance (*type* of camera surveillance) using local cameras (type of surveillance *camera*).

A look at the different operational aspects of each type of camera should help clarify the ethical issues involved. To this end, the surveillance camera typology defined by the *Association sur l'accès et la protection de l'information* (AAPI)[142] is worthy of consideration.

It should be noted that camera types could also be combined. Camera surveillance could therefore be:

- Used in real time, cameras being connected to a monitoring station that receives images on a closed circuit monitor. Operators intervene when needed;
- Passive in nature, recordings are viewed at regular intervals;
- Active in nature, i.e. involve continuous viewing by security staff;
- Used with continuous recording for general or specifically targeted surveillance;
- Concealed, when conducted without the subject's knowledge;
- Open, when the presence of cameras is publicly visible and explicit information about their use is clearly visible.

135. Michel LAPORTE, op. cit., p. 19.
136. OFFICE OF THE PRIVACY COMMISSIONER OF CANADA, *OPC Guidelines for the Use of Video Surveillance of Public Places by Police and Law Enforcement Authorities*, March 2006, available at <http://www.privcom.gc.ca/information/guide/vs_060301_e.asp>
137. FREEDOM OF INFORMATION AND PROTECTION OF PRIVACY, *Guide to Using Surveillance Cameras in Public Areas*, Gouvernment of Alberta, June 2004, available at <http://foip.gov.ab.ca/resources/publications/pdf/SurveillanceGuide.pdf>
138. OFFICE OF THE INFORMATION & PRIVACY COMMISSIONER FOR BRITISH COLUMBIA, *Public Surveillance System Privacy Guidelines*, 26 January 2001, available at <http://www.oipcbc.org/advice/VID-SURV(2006).pdf>
139. OFFICE OF THE SASKATCHEWAN INFORMATION AND PRIVACY COMMISSIONER, *Guidelines for Video Surveillance by Saskatchewan Public Bodies*, 24 June 2004, available at <www.oipc.sk.ca/webdocs/VideoSurveillance.pdf>
140. Ann CAVOUKIAN, *Guidelines for Using Video Surveillance Cameras in Public Spaces*, Information and Privacy Commissioner/Ontario, October 2001. <www.ipc.on.ca/images/Resources/video-e.pdf>
141. Michel LAPORTE, op. cit., pp. 17-18.
142. ASSOCIATION SUR L'ACCÈS ET LA PROTECTION DE L'INFORMATION, *L'utilisation de caméras de surveillance par des organismes publics dans des lieux publics*, Memoir presented to the Commission d'accès à l'information during its public consultation, September 2003.

Moreover, there are different types of surveillance cameras. The Commission bases its description of these on the report presented by the Canadian Security Association (CANASA)[143] during the course of the CAI consultation, and included in their report[144].

First, a distinction should be drawn between local, monitoring, ID, covert and zoom-tilt-pan cameras.

Local cameras are used to monitor a specific location. Since the object of attention is on a place rather than specific people, this type of equipment would not likely be used to identify an individual. This is the most widely used type of camera and is mostly used to monitor crowds.

Monitoring cameras are mostly used to monitor roadways since they offer a panoramic view.

ID cameras are most often built into ATM machines and banks. These are primarily used to identify individuals traveling through a specific location.

Covert cameras are used to secretly monitor certain areas. They can be used to capture specific events when tracing or tracking individuals or during police investigations. These fixed cameras can be as small as a pencil tip.

Zoom-tilt-pan cameras feature programmable viewing angles to avoid capturing unwanted areas, such as public streets or private homes. They can be used to monitor locations such as marshalling yards.

Video surveillance applications

It is easy to get lost in the sheer number and diversity of video surveillance applications and purposes when attempting to map out the use of this technology. The Commission, once again based on the work of the CAI, has determined that public security applications are without a doubt the most common. Moreover, crime prevention and the fight against insecurity are the most often cited reasons for their use[145].

Among other video surveillance applications, motor vehicle traffic monitoring is also worthy of mention. The purpose here is to "quickly detect an incident or congestion problem so as to minimize their impact, to reduce the occurrence of secondary accidents and user travel time, to provide real time information to drivers and ensure close collaboration with emergency service providers[146]". Private citizens are also interested in video surveillance equipment for their personal use. Here, applications can vary considerably; from monitoring aged parents in retirement homes to make sure they receive proper treatment, to spying on a babysitter when parents are away (nanny cams), etc. Private businesses also use this technology in an effort to reduce and deter theft and vandalism-related losses, for example.

Current and future technologies and their method of operation

As mentioned above, recent advances in technology have expanded the range of possible video surveillance applications. Digitization of captured images has revolutionized the field: Data collection, storage and handling now have unprecedented reach, particularly with the help of information and communications technology. Other innovations testify to video surveillance's position at the leading edge of technology: "miniature cameras, cameras that tilt 360º, biometric units that record facial properties, high-resolution, night vision, electromagnetic devices that can see through material, infrared equipment that detect temperature changes, low dose x-rays that provide images of bodies and what they carry[147]".

Among the current and future technologies under consideration, facial recognition and intelligent software raise ethical issues, particularly with respect to privacy, the risk of discrimination and stigmatization and the respect for democracy.

143. CANADIAN SECURITY ASSOCIATION, *Pour un monde en toute sécurité*, Memoir presented to the Commission d'accès à l'information, 2 September 2003.
144. Michel LAPORTE, op. cit., p. 54.
145. Ibid., p. 15.
146. Ibid., p. 16.
147. FÉDÉRATION DES TRAVAILLEURS ET TRAVAILLEUSES DU QUÉBEC, *Mémoire de la Fédération des travailleurs et travailleuses du Québec présenté à la Commission d'accès à l'information du Québec sur l'utilisation de caméras de surveillance par des organismes publics dans les lieux publics*, Montréal, 22 September 2003, p. 7, available at <http://www.ftq.qc.ca/modules/documents/index.php?id=5&langue=fr>.

Facial recognition allows for the comparison of the captured image of an individual with the facial images of wanted individuals or alleged terrorists, for example.

Intelligent software contains algorithms that could enable the detection of behaviour considered unacceptable or deviant. For example, intelligent software could detect a person walking against the flow of a moving crowd, as this behaviour deviates from the norm. The selection of behaviours to be given special attention is left up to the surveillance camera user. Moreover, a police force could personalize intelligent software to pick up behaviours associated with the sale of illegal drugs, or a subway security service could target individuals loitering behind after a train has left a station.

These new technologies highlight the fact that machines are increasingly replacing humans in video surveillance data analysis. In its preface to its guidelines for the use of video surveillance, the Office of the Privacy Commissioner of Canada offers this insight into the ethical impact of these new technologies:

> *When video surveillance was done with tapes, where an operator had to watch each event to make a judgement about an individual, the volume of work kept misuse down to a minimum. Now we have facial recognition systems and pattern recognition software that can massage the vast stream of images, so the actual use of the data increases, even if it is not by human operators. The likelihood of images being retained for further data mining increases simply because the workload is now potentially manageable. The risk of systematized observations of groups or persons now exists, simply because it is technically feasible*[148].

Incorporating ethics into NSMT programming procedures thus constitutes a major challenge, especially when decisions are made by machines rather than by humans. This ethical issue will be further considered below.

The benefits of video surveillance

The digital revolution has imparted video surveillance with significant benefits, particularly with respect to efficiency and cost-reduction. For instance, data storage (many viewing hours can be stored on a single CD) and camera networks (surveillance camera networks can be interconnected with potential remote access via the Internet) represent significant user savings. This partly results from the fact that machines end up taking over surveillance duties: Instead of paying police officers and on-site security guards, some organizations prefer to purchase video surveillance equipment.

Proponents of video surveillance hail its alleged ability to reduce crime by dissuasion as its main benefit. This effect is even more desirable in the fight against terrorism:

> *The use of video surveillance to detect, deter and prosecute crime has increased significantly over the last few years—in Canada and abroad. Police and law enforcement authorities increasingly view it as a legitimate tool to combat crime and ward off criminal activity—including terrorism. Recent events have heightened the interest of public authorities in deploying video-surveillance in public places. It is widespread in the United Kingdom and increasingly used by law enforcement and anti-terrorism authorities in the U.S. and Canada, particularly since September 2001*[149].

Others, however, challenge these claims and point to problems with video surveillance.

The drawbacks of video surveillance

In question is not so much the reliability of the equipment but the dissuasiveness of video surveillance. According to a British meta-analysis, video surveillance has a relatively small effect in reducing crime[150]. A number of additional details must be considered. Although most studies tend to demonstrate a dissuasive effect, others, though fewer in numbers show an opposite effect[151]. Furthermore, video surveillance effectiveness varies according to the nature of the crime committed, proving effective against car theft, but not against violent crimes[152].

The geographic and urban impact of a massive implementation of this type of technology on delinquency remains subject to debate. Until convincing scientific

148. OFFICE OF THE PRIVACY COMMISSIONER OF CANADA, op. cit.

149. Ibid.

150. Brandon C. WELSH and David P. FARRINGTON, *Crime Prevention Effects of Closed Circuit Television: A Systematic Review*, Home Office Research Study 252, August 2002, p. 41, available at <http://www.homeoffice.gov.uk/rds/pdfs2/hors252.pdf>.

151. Ibid.

152. Ibid., p. 42.

evidence sheds light on the subject, the Commission ponders the risk of crime displacement: Does the surveillance of a specific location to deter crime encourage criminals to migrate towards less monitored areas?

Finally, if video surveillance can have a dissuasive effect on some criminals, it must be assumed that would-be terrorists who are willing to give up their lives in an attack would hardly be concerned about being filmed and recognized. At best, surveillance cameras could record terrorists before they perpetrate their attacks (which could help thwart their efforts), or during and after an attack, which could help authorities identify the attackers, or find them if they managed to survive.

The video surveillance market

The future of the video surveillance market is likely to grow, particularly due to concerns over potential terrorist attacks, but also due to the fact that many organizations are likely to replace their current equipment with IP technology[153]. Consequently, the world video surveillance market should grow by 37% between 2006 and 2009[154].

Public interest in video surveillance

Generally speaking, public opinion is favourable to the use of surveillance cameras for security purposes. Admittedly, it is reassuring to know that public spaces are monitored and that assistance would be provided should an incident occur. Moreover, since most people claim to have done nothing wrong, they remain somewhat indifferent to the use of video surveillance. A May 2004 *La Toile de Sherbrooke* survey reports an 82% approval rate among respondents for the use of video surveillance for security purposes. In a more recent survey[155], respondents were asked to indicate their level of support for various anti-terrorist measures. Installation of surveillance cameras in all public spaces received 72% support. For Québec alone, this figure climbs to 77%.

In Europe, the majority a respondents in a major study across five countries voiced their approval of video surveillance in their city[156]. The degree of acceptance, however, varies significantly according to the context within which these cameras are to be used: High levels of acceptance for places such as financial institutions and public transportation, and little to none for more private places such as changing-rooms[157].

Radio frequency identification (RFID): Towards ambient intelligence?

Radio frequency identification (RFID) technology applications are both many and diverse. To describe them in a few words would be an impossible task. In addition, the very nature of this technology, that is, an enabler of functionalities that does not limit its use to one specific application[158], further complicates their analysis. Once again, for the purposes of this Position statement, RFID will be considered with respect to its security applications. Other purposes may, however, be mentioned in passing when relevant. First, a few definitions are presented in order to better understand RIFD purposes and operations.

Some useful definitions

RFID involves two main components. First, a tag containing "an electronic circuit that stores data and an antenna which communicates the data via radio waves[159]" is required. This tag then communicates with

153. 'Research: World CCTV Market to Grow 37 Percent by 2009', *SecurityInfoWatch.com*, 14 July 2006. <http://www.securityinfowatch.com/online/Research--Studies-and-Whitepapers/8702SIW321>.

154. Ibid.

155. STRATEGIC COUNSEL, *Immigration, Terrorism and National Security*, 7 August 2005.

156. Leon HEMPEL and Eric TÖPFER, *CCTV in Europe, Final Report*, Working Paper No. 15, August 2004, p. 42. available at <http://www.urbaneye.net/results/ue_wp15.pdf>.

157. Ibid.

158. EUROPEAN COMMISSION, *Your Voice on RFID. Background Document for Public Consultation on Radio Frequency Identification (RFID) – Summary of Five Workshops*, July 2006, p. 6, available at <http://www.rfidconsultation.eu/docs/ficheiros/Your_voice_on_RFID.pdf>.

159. WORKING PARTY ON THE PROTECTION OF INDIVIDUALS WITH REGARD TO THE PROCESSING OF PERSONAL DATA, *Working Document on Data Protection issues Related to RFID Technology*, Brussels, January 19, 2005, p. 3, available at <http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2005/wp105_en.pdf>.

a reader, which includes "an antenna and a demodulator which translates the analogue information [...] into digital data. The digital information can then be processed by a computer[160]."

The purposes of RFID

The end purposes of RFID are so numerous that only the most common will be mentioned. For security purposes, RFID has recently begun to be used in identity documents such as passports. RFID tags used in American passports[161] and those of several members of the European Union[162] contain biometric data that can be scanned at border stations. These applications are mainly used to deter document fraud and identity theft. Access control to regulated areas (such as airports) constitutes another RFID application[163]. Using access cards with RFID tags, authorized individuals are allowed to enter restricted areas.

Current and future technologies and their method of operation

RFID involves an electronic tag with a miniature antenna that can be activated by a specific reader to which it then communicates information. This technology is passive, i.e. the tag does not have its own power source. It is activated by the radio frequencies sent by the RFID reader, and uses energy from the radio signal to respond. This is the most widely used method of operation. Active RFID tags feature an internal battery and a wider read range depending on the reader being used[164].

RFID tags come in many shapes and sizes[165]. Some are quite obvious, such as theft control tags attached to clothing in some retail stores. Others can be the size of a grain of rice and placed under the skin, and used for pets and endangered species. Finally, continuing efforts are made to develop tags so small they could be incorporated into dollar bills in order to deter counterfeiting.

The transfer of data from a RFID tag to a reader can be done using four types of frequencies[166]:

- Low frequency (100-500 kHz). Read range is less than a metre. This technology requires a fairly large and expensive antenna, and is mainly used for access control and animal tagging.
- High frequency (10-15 MHz). Read range is approximately one metre. This technology is more widely used, mainly for access control; retail merchandise tagging, libraries and transport.
- Ultra-high frequency (850-1000 MHz) – Read range varies from four to five metres. This technology, which will likely replace high frequency, is mostly used in inventory management.
- Microwave (2,4-5,8 GHz) – Read range approximately one metre. This technology is highly susceptible to interference, which limits its use to speed passes.

The operation and applications of RFID have a direct impact on their potential normative framework. Given that this technology is still in the stages of development, some suggest that the industry should regulate itself. Such guidelines could complement existing laws that govern the management of personal information[167]. Obviously, this type of arrangement would considerably limit the possibility of levying sanctions on delinquent users. For this reason, some suggest the creation of a special ombudsman to deal with consumer complaints about products using RFID tags[168].

160. Ibid.
161. DEPARTMENT OF STATE, 'Department of State Begins Issuing Electronic Passports to the Public', Press release, 14 August 2006.
162. Guillaume DELEURENCE, 'Le passeport se convertit à l'électronique, avant la biométrie', *01net.com*, 28 August 2006. <http://www.01net.com/editorial/324183/societe/le-passeport-se-convertit-a-l-electronique-avant-la-biometrie/>.
163. WORKING PARTY ON THE PROTECTION OF INDIVIDUALS WITH REGARD TO THE PROCESSING OF PERSONAL DATA, p. 5.
164. COMMISSION D'ACCÈS À L'INFORMATION DU QUÉBEC, *Radiofrequency Indentification Technology (RFID): Is there Reason to Mistrust It?*, Analytical Document, May 2006, p. 1, available at <http://www.cai.gouv.qc.ca/06_documentation/01_pdf/RFID_en.pdf>.
165. ELECTRONIC PRIVACY INFORMATION CENTER, 'Radio Frequency Identification (RFID) Systems', *epic.org*, 13 January 2006. available at <http://www.epic.org/privacy/rfid/>.
166. Teresa SCASSA *et al., An Analysis of Legal and Technological Privacy Implications of Radio Frequency Identification Technologies*, prepared for the Privacy Commissioner of Canada, 28 April 2005, p. 6.
167. EUROPEAN COMMISSION, *Your Voice on RFID. Background Document for Public Consultation on Radio Frequency Identification (RFID) – Summary of Five Workshops*, July 2006, p. 14, available at <http://www.rfidconsultation.eu/docs/ficheiros/Your_voice_on_RFID.pdf>.
168. Ibid.

RFID applications vary somewhat with regards to personal data. If the introduction of tags containing biometric data on passports constitutes a clear example requiring legislation regarding the protection of personal data, other RFID applications may not.

The Working Party on the Protection of Individuals with Regard to the Processing of Personal Data of the European Parliament and of the Counsel (named Working Party 29) ponders this issue in the following question:

> *It may then be asked whether this means that the data protection Directive necessarily applies to the collection of data through RFID technology. The answer will depend in general on the specific concrete application of RFID technology, particularly on whether the specific RFID application entails the processing of personal data as defined by the general DP Directive*[169].

The benefits of RFID

As with other newly emerging technologies, RFID applications give birth to a host of promises. RFID could be used to help improve consumer product distribution logistics, better merchandise tracking, theft prevention, and more efficient counterfeit detection[170]. Unlike conventional bar codes, RFID tags can be scanned from a distance, as well as through snow, fog, ice, or even paint, which further contributes to their appeal and reliability[171].

In the near future, RFID could be used to track individuals in time and space. Police authorities, among others, would greatly benefit from this type of surveillance capability. RFIDs implanted into the human body also promise many benefits: These tiny but durable tags could contain information on the identity, physiological features, health and nationality of their holder[172].

The drawbacks of RFID

Just as electronic passports with RFID tags containing biometric information were first issued, some document security experts began to detect major flaws in RFID tags that allowed stored information to be duplicated and identical passports to be produced[173]. This outcome, and the expected expanded use of RFID tags in other identity documents, has revived previously held concerns about the risk of fraud. The absence of encryption technology in RFID tags casts further doubts on the ability to adequately protect stored information.

In Québec, the CAI has also raised questions regarding the impact of adding RFID tags to identity documents: "It is also appropriate to consider whether the incorporation of RFID chips containing personal information into the driver's permit or passport could increase the risks of identity theft[174]."

Another major flaw is closely related to one of RFID's main benefits. Remote scanning opens the door to wrongful tracing and tracking: An unauthorized individual could read the contents from a distance without the holder's knowledge[175]. With respect to security, and considering terrorists' desire to target their attacks, this could help terrorists "select" potential victims from a crowd based on nationality, for instance[176].

Deception and trickery could also be used to circumvent RFID systems[177]: An ill-intentioned individual could feed wrong information to either a reader or RFID tag, or perpetrate a Denial of Service (DoS) attack, rendering the system inoperable.

169. WORKING PARTY ON THE PROTECTION OF INDIVIDUALS WITH REGARD TO THE PROCESSING OF PERSONAL DATA, op. cit., p. 8.
170. EUROPEAN COMMISSION, *RFID Security, Data Protection and Privacy, Health and Safety Issues*, Policy Framework Paper, 11 May 2006, <http://www.rfidconsultation.eu/41/38/264.html>.
171. ELECTRONIC PRIVACY INFORMATION CENTER, op. cit.
172. Kenneth R. FOSTER and Jan JAEGER, 'RFID Inside. The Murky Ethics of Implanted Chips', in *IEEE Spectrum*, March 2007, p. 27, available at <http://pages.cs.wisc.edu/~markhill/cs252/Spring2007/handouts/spectrum07_rfid_ethics.pdf>.
173. Kim ZETTER, 'Hackers Clone E-Passports', *Wired.com*. 3 August 2006. <http://www.wired.com/science/discoveries/news/2006/08/71521>.
174. COMMISSION D'ACCÈS À L'INFORMATION DU QUÉBEC. *Radiofrequency Identification Technology (RFID): Is there Reason to Mistrust It?*, Analytical Document, May 2006, p. 4 available at <http://www.cai.gouv.qc.ca/06_documentation/01_pdf/RFID_en.pdf>
175. WORKING PARTY ON THE PROTECTION OF INDIVIDUALS WITH REGARD TO THE PROCESSING OF PERSONAL DATA, op. cit., p. 7.
176. Ibid.
177. EUROPEAN COMMISSION, RFID *Security, Data Protection and Privacy, Health and Safety Issues*, Policy Framework Paper, 11 May 2006, p. 9, available at <http://www.rfidconsultation.eu/41/38/264.html>.

It is therefore important to note that radio frequency technology is not 100% accurate, and that other support systems, such as databases, are just as prone to attack. According to the European Commission, further research and development are required for certain applications[178]. Overall, RFID technology remains at the development stage.

The RFID market

Although RFID technology has been around since World War II, only recently, due to improvements in technology, has the market begun to expand significantly. A total of 2.5 billion tags were sold between 1946 and 2006, including 600 million sold in 2005 alone[179]. Sales of 1.3 billion tags were expected for 2006[180]. In terms of market share, passive tags represent three quarters of all tags sold; active tags cover the remaining quarter[181].

If the industry can meet the number of challenges presented by this technology, such as high cost of production, reliability and frequency compatibility, the market should grow at an exponential rate: A 2.7 billion dollar US market in 2006 could grow to 26.2 billion dollars by 2016[182].

In 2004, security applications covered the lion's share of the RFID market[183]. Since then, inventory management applications have increased substantially. Industry observers predict a drop in the cost of RFID manufacturing, which should lead to increased use in individual labelling of medication, animals, luggage, books, etc[184].

Public interest in RFID

Recent American and European studies suggest that the general public has not yet formed a decisive opinion on RFID technology, and wants to find out more[185]. The European Commission has come to the same conclusion, and seeing that consumers are not sufficiently aware of the possible invasion of privacy by new technologies such as RFID, it has recommended that an information campaign be held on the matter[186].

From a consumer point of view, respondents see potential benefits in the use of RFID, but also apprehend a negative side. On one hand, RFID are expected to help recover stolen objects more quickly, be built into motor vehicle anti-theft devices, help improve food safety, reduce production costs, and consequently, the price of consumer products[187].

On the other hand, American and European consumers are concerned that RFID might facilitate third party use of their information, an upsurge in marketing campaigns, and the potential to track consumers through their various purchases[188]. Health and environmental issues are secondary concerns in the minds of respondents.

* * *

178. EUROPEAN COMMISSION, *Your Voice on RFID. Background Document for Public Consultation on Radio Frequency Identification (RFID) – Summary of Five Workshops*, July 2006, available at <http://www.rfidconsultation.eu/docs/ficheiros/Your_voice_on_RFID.pdf>.
179. IDTECHEX, *RFID Forecast, Players & Opportunities 2006-2016*, October 2006.
180. Ibid.
181. EUROPEAN COMMISSION, *RFID Security, Data Protection and Privacy, Health and Safety Issues*, Policy Framework Paper, 11 May 2006, p. 9. <http://www.rfidconsultation.eu/41/38/264.html>.
182. IDTECHEX, op. cit.
183. EUROPEAN COMMISSION, *RFID Security, Data Protection and Privacy, Health and Safety Issues*, Policy Framework Paper, 11 May 2006, p. 9. <http://www.rfidconsultation.eu/41/38/264.html>.
184. Ibid.
185. CAP GEMINI ERNST & YOUNG, *RFID and Consumers. Understanding Their Mindset, A U.S. Study Examining Consumer Awareness and Perceptions of Radio Frequency Identification Technology*, Executive Summary, 13 January 2004, p. 2, available at <http://www.rfidconsultation.eu/docs/ficheiros/CPRD_RFID_mindset_ES.pdf> and Helen DUCE, Executive Briefing, Public Policy: Understanding Public Position statement, Auto-ID Centre, 1 February 2003. <http://www.autoidlabs.org/single-view/dir/article/6/199/page.html>.
186. EUROPEAN COMMISSION, *Your Voice on RFID. Background Document for Public Consultation on Radio Frequency Identification (RFID) – Summary of Five Workshops*, July 2006, p. 15, available at <http://www.rfidconsultation.eu/docs/ficheiros/Your_voice_on_RFID.pdf>.
187. CAP GEMINI ERNST & YOUNG, op. cit., p. 2.
188. Ibid.

A separate and individual consideration of NSMT necessarily excludes an important dimension, and consequently limits the scope of the Commission's analysis: The convergence of NSMT in security systems. Examples of current convergent applications include facial recognition software (biometrics) combined with images captured by a surveillance camera (video surveillance), or the inclusion of biometric data in RFID tags in passports. According to experts, risks involved by converging NSMT are not merely added but multiplied.

Chapter 3
An ethical look at new surveillance and monitoring technologies: In search of a balance in values

The deployment of new surveillance and monitoring technologies (NSMT) reveals in good measure the importance of the fundamental values shared by democratic societies. In a context where societies are plagued by a sense of insecurity that is regularly fuelled by the media, and where risk and surveillance are prominently featured, an ethical look at the deployment of NSMT is essential. The Commission has therefore selected the following issues for consideration: Assessment of the relevance, effectiveness and reliability of NSMT, the proportionality of response to insecurity, social acceptability, consent, respect for the end purpose, and the protection of personal information.

Following the events of September 11th, 2001, a number of security measures have been implemented and have further empowered governments, police forces and the legal system to gather much more detailed personal information than ever before, and to use this information for purposes other than for which it was initially obtained[189]. In addition to this trend are the actions of private actors who are particularly interested in better and more efficient security systems. This tendency illustrates how the value of security is significantly increasing in importance, perhaps to the detriment of other values that are fundamental to democratic societies, such as individual freedom. In the realm of security, the values of security and freedom are often in conflict. A compromise, however, is not impossible.

One must exercise caution when discussing a shift in balance between powers of the state and individual freedoms. These concepts cannot be quantified nor can they consequently be balanced "mathematically". Inasmuch as a loss of freedom can be real and tangible, corresponding resulting gains in security are much more vague and uncertain.

These considerations call for a careful examination of the moral justification behind any compromise to individual rights and freedoms, especially since doing so under a particular set of possibly temporary circumstances remains risky, these rights being very difficult to recover later down the road.

The image of balance should not be seen as anything other than what it is: The representation of an eminently complex phenomenon. In fact, no image could perfectly render the close inter-relationships that exist between freedom and security. These two values are fundamental to democratic life, and each can potentially curtail or promote the other. For the purposes of this Position statement, this phenomenon can be illustrated as follows: The emergence of NSMT is closely linked to a desire by the state and other organizations to ensure greater security for their territory. The state, in exercising this power, aims to preserve democracy, but paradoxically, also encroaches on the fundamental rights and freedoms that represent democratic societies. Although it must be recognized that NSMT can help ensure better security, their deployment must also aim to maintain respect for individual rights and freedoms.

A great divide exists between the ideal of promoting security and freedom, where one is not favoured at the expense of the other, and the reality that a choice must be made between these two values. The Commission, harbouring a preference for the simultaneous promotion of both values, recognizes that in the vast majority of situations, some form of arbitration, compromise or balance must be reached. The challenge is to find this proper balance.

189. INSTITUTE FOR PROSPECTIVE TECHNOLOGICAL STUDIES, op. cit., p. 4.

Finally, the Commission wishes to draw attention upon the underlying risk of loss of autonomy in the deployment of NSMT. Individuals can change their behaviour once they become aware they are under surveillance. Thus, if they know they will be the object of video surveillance, individuals could fear reprisals after participating in public demonstrations or openly criticizing government decisions. Consequently, not only are their rights and freedoms threatened, but their autonomy, the very expression of their liberty as well.

Assessment of the relevance, effectiveness and reliability of NSMT

In order to be legitimately deployed, NSMT must not only prove harmless to health, but also be relevant, effective and reliable. To be relevant, NSMT must be determined as the best method of achieving a recognized security objective. Alternatives that are less intrusive to privacy should be favoured. In order for NSMT to be effective, they must produce results that match initial goals. In addition, NSMT must be reliable, that is, their use must not present more problems than solutions.

In order to justify the deployment of NSMT, they must reach a higher degree of relevance, effectiveness and reliability. The main flaws pertaining to each of the technologies considered in this Position statement are presented in chapter 2. How should relevance, effectiveness and reliability be determined? Who should be responsible for this assessment? The promoters? Public authorities? These technical questions need answers. Assessment mechanisms and their results must be made available to the public and easy to understand. The value of transparency towards the public is of utmost importance.

Although the general public has confidence in technology and its information processing capabilities, it should be noted that computer programs that process data collected by NSMT can contain errors or be corrupted[190]. Moreover, it would be a mistake to characterize NSMT used for security purposes as invulnerable. The deployment of technology perceived as reliable that would contribute to promoting a false sense of security among the public would be unacceptable.

The Commission thus calls on all concerned to reflect on the assessment of the relevance, effectiveness and reliability of NSMT. It also wishes to recall the importance of deploying effective and reliable technologies so as to avoid causing harm to innocent people. The more NSMT are known to be relevant, effective and reliable, the more difficult it will be for suspects to prove their innocence. The Commission is also concerned that a reversal of the burden of proof could become the rule rather than the exception if NSMT are to be used for purposed of identifying suspects.

Proportionality of response to insecurity: For a moderate deployment

Considering comments made in Chapter 1 with regards to a public sense of insecurity and given the fact that Canada is a generally safe country, the response to insecurity through NSMT should not reach disproportionate levels. In concurrence with the *Comité consultatif national d'éthique pour les sciences de la vie et de la santé (CCNE)*, the Commission feels that the "proportionality of means concept[191]" must be taken into consideration not only with regards to biometric systems, but with NSMT in general. Implementation of surveillance methods that are too intrusive, considering their end purpose and context, just as "integrating personal data beyond their declared purpose[192] is unjustifiable. It is therefore important that NSMT deployment be moderate and calibrated to real security needs as opposed to a direct response to feelings of insecurity triggered by spectacular events such as terrorist attacks. The Commission calls on decision-makers in both the public and private sectors to conduct a careful and lucid assessment of NSMT needs for security purposes.

190. UNESCO, *Ethical Implications of Emerging Technologies: A Survey*, (Paris: UNESCO, 2007), p. 14, available at <unesdoc.unesco.org/images/0014/001499/149992E.pdf>.

191. COMITÉ CONSULTATIF NATIONAL D'ÉTHIQUE POUR LES SCIENCES DE LA VIE ET DE LA SANTÉ, *Biométrie, données identifiantes et droits de l'homme*, Position statement n° 98, 26 April 2007, p. 14, available at <www.comite-ethique.fr/docs/fr/avis098.pdf>.

192. Ibid.

It is essential that an evaluation of the relationship between technical reliability, proportionality of response to insecurity and the degree of intrusiveness be conducted for each and every NSMT deployment. It appears that such an evaluation would in itself allow for insights into the ethics behind the end purpose to which NSMT are deployed. Such a groundbreaking procedure would help Québec assume a leadership role in evaluating the ethics involved in the use of this type of technology.

Moreover, at the heart of the assessment of the proportionality of the response to insecurity lie players who are all too often ignored by private and public decision-makers: NSMT providers and fitters. These players are on the front line in that they must directly meet the technical security needs of private and public organizations and citizens. In addition to providing appropriate advice to their clients on the use of NSMT, they must be prepared to answer the following question: Which technology is best suited to ensure a given level of security? In other words, which security system is best recommended to meet their security requirements? These providers and fitters are the first to be confronted by the ethical issues raised by the Commission. It is also necessary that they be sensitized to the ethical questions involved in their practices if the deployment of NSMT is to be consistent with the promoted values. The central question appears to revolve around the issue of how to achieve proportionality of response to insecurity in a context of very rapid market growth where an emphasis on profit often overshadows ethics. These considerations suggest a need for a deeper analysis of NSMT regulation. The results could then be distributed among key players through subsequent legislative developments.

In Québec, the new Private Security Act specifically oversees "activities related to electronic security systems, namely, installing, maintaining and repairing, and ensuring the continuous remote monitoring of, burglar or intrusion alarm systems, video surveillance systems and access control systems, except vehicle security systems […][193]". The Act further stipulates that the future *Bureau de la sécurité privée* will provide training to representatives of licensed agencies and that the Government could, by regulation, determine which training is appropriate in order to use certain equipment, or which training credentials are required for the deliverance of an agent licence[194]. This training should include a section focused on ethical issues. Hence:

The Commission recommends that training provided by the *Bureau de la sécurité privée* to representatives of licensed agencies include a compulsory ethics component based on the ethical issues raised in this Position statement and that the Government, in compliance with the Private Security Act, adopt the necessary regulations so that the training required for the deliverance of an agent licence also include an ethics component.

Social acceptability: An essential condition

The deployment of NSMT and their ongoing technological development often seem unavoidable. Such a perception underlies the fact that these events occur without any particular debate. In its Position statement on biometrics, the *Comité consultatif national d'éthique pour les sciences de la vie et de la santé* feels that "[t]he first ethical issue arises from the unavoidability factor that is felt without a serious debate on the potential risks and abuses that could result from this evolution[195]". This unavoidability factor is often perceived as emanating from pressure for greater economic efficiency, which all too often precludes taking the time to look at the values involved and especially the type of society in which we want to live[196].

Considering the current popularity of governments that have made security their key issue and in the light of the results of polls and surveys on public acceptance of NSMT, it would appear that NSMT deployment is not contrary to popular will. The Commission, however, raises questions as to the levels of public awareness with regards to biometrics, video surveillance and radio frequency identification (RFID). In addition, any form of consultation on NSMT should place a premium on public participation and seek, above all, to receive informed and enlightened opinions.

193. R.S.Q., chapter S-3.5, 2006, c. 23, s. 1.

194. R.S.Q., chapter S-3.5, 2006, c. 23, s. 41, 111 and 112.

195. COMITÉ CONSULTATIF NATIONAL D'ÉTHIQUE POUR LES SCIENCES DE LA VIE ET DE LA SANTÉ, op. cit., p. 17.

196. David H. FLAHERTY, op. cit., p. 6.

Consent: A challenging concept for NSMT

In most cases, it is simply impossible for individuals under surveillance to give their consent. In fact, individual free and clear consent is simply not a concept that can be applied to NSMT. This statement of fact is not, however, above raising ethical questions.

With respect to biometrics, "consent and transparency (could) be optional in certain biometric applications[197]". How is this possible? People constantly leave their fingerprints on everything they touch, lose hair (DNA), speak out loud (voice recognition), and use computers (keystroke dynamics). These elements can all easily be collected and used to extract biometric information. The potential for collecting biometric data without an individual's knowledge (and thus without their consent), raises concerns about the insidious emergence of a surveillance society within which the power to manage the disclosure of one's personal information, and therefore individual autonomy, is slowly eroded[198].

With video surveillance, consent is simply not applicable. In fact, the only way for individuals to deny consent to video surveillance is to avoid places that use surveillance cameras[199]. Given the widespread use of surveillance cameras in public and private spaces, this option cannot seriously be considered.

Several organizations have commented on the issue of consent to radio frequency identification. Working Party 29 has closely examined RFID technology through the European Directive with respect to personal information. The group underscores the primary role of consent from a legal standpoint with RFID: "Under most of the scenarios where RFID technology is used, consent from individuals will be the only legal ground available to data controllers to legitimise the collection of information through RFID […][200]."

The Act respecting access to documents held by public bodies and the protection of personal information states the following:

A person who collects personal information verbally from the person to whom it relates on behalf of a public body must introduce himself and, when information is first collected and subsequently on request, inform that person

1) *of the name and address of the public body on whose behalf the information is being collected;*
2) *of the purposes for which the information is collected;*
3) *of the categories of persons who will have access to the information;*
4) *of the fact that a reply is obligatory, or that it is optional;*
5) *of the consequences for the person concerned or, as the case may be, for the third person, in case of a refusal to reply;*
6) *of the rights of access and correction provided by law*[201].

Moreover, it should be mentioned that this section is subject to certain restrictions, particularly with respect to the deployment of NSMT for security purposes: "This section does not apply to judicial inquiries or to any investigation or report made by a body responsible by law for the prevention, detection or repression of crime or statutory offences[202]."

Québec has nevertheless made a provision for consent to the use of biometrics:

> *Section 44 of the Act to establish a legal framework for information technology states that the verification or confirmation of a person's identity through biometric characteristics is not permitted without the person's "express consent". Let us stress that a person's consent to the recording of biometric characteristics does not permit one to disregard the obligation of necessity (e.g. that the*

197. ORGANISATION FOR ECONOMIC CO-OPERATION AND DEVELOPMENT, op. cit., p. 4.
198. John D. WOODWARD Jr. *et al., Army Biometric Applications: Identifying and Addressing Sociocultural Concerns*, RAND, 2001, p. 25, available at <http://www.rand.org/publications/MR/MR1237/>.
199. Leon HEMPEL and Eric TÖPFER, op. cit., p. 66.
200. WORKING PARTY ON THE PROTECTION OF INDIVIDUALS WITH REGARD TO THE PROCESSING OF PERSONAL DATA, op. cit., p. 10.
201. R.S.Q., chapter A-2.1, 1982, c. 30, s. 65; 1990, c. 57, s. 15; 2006, c. 22, s. 36.
202. Ibid.

type of information be judged necessary) as provided in section 64 of the Act respecting access to documents held by public bodies and the protection of personal information and sections 4 and 5 of the Act respecting the protection of personal information in the private sector. In other words, a public body is not allowed to collect biometric data if this data is not necessary for the exercise of its powers or the implementation of a program under its management. Obtaining consent does not forgoe this limitation. The same goes for a private organization which may collect only the information necessary for the object of the file established on a person[203].

Within the framework of the Act Respecting the Protection of personal information in the private sector, consent is considered as follows: "Consent to the collection, communication or use of personal information must be manifest, free, and enlightened, and must be given for specific purposes. Such consent is valid only for the length of time needed to achieve the purposes for which it was requested[204]."

In addition, section 8 states that:

A person who collects personal information from the person concerned must, when establishing a file on that person, inform him:

1° of the object of the file;

2° of the use which will be made of the information and the categories of persons who will have access to it within the enterprise;

3° of the place where the file will be kept and of the rights of access and rectification[205].

With respect to the disclosure of personal information, sections 67, 67.1, 67.2, 68 and 68.1 of the Act respecting access to documents held by public bodies and the protection of personal information provide for certain exceptions to the obligation to obtain an individual's consent for the disclosure of personal information that relates to them.

For example, section 68 states that:

A public body may, without the consent of the person concerned, release personal information

1° to a public body or an agency of another government if it is necessary for the exercise of the rights and powers of the receiving body or the implementation of a program under its management;

1.1° to a public body or an agency of another government if it is clearly for the benefit of the person to whom it relates;

2° to a person or a body where exceptional circumstances justify doing so;

3° to a person or body if it is necessary for the purposes of a service to be provided to the person concerned by a public body, in particular for identifying the person.

Such provisions open the door to the disclosure of personal information without the knowledge of the concerned individual. Once consent is given for the collection of information by NSMT, this information can be disclosed to others without further consent on the part of those concerned, in violation of their autonomy. Although certain conditions must be met before any information is disclosed, some of these remain somewhat vague and susceptible to abuse.

The stealthy nature of NSMT used in many areas of everyday life is also a source of concern. The goal of many NSMT promoters, in fact, is to blend them into the environment to make them invisible. This practice could have repercussions on personal autonomy and privacy.

Although individual consent does not apply to NSMT, personal autonomy, and as such, the fundamental values of democratic societies must be respected. In the spirit of the principle of representation, by virtue of which elected officials make political decisions rather than the public as a whole, the Commission believes that if the deployment of NSMT is done in a manner that is

203. COMMISSION DE L'ÉTHIQUE DE LA SCIENCE ET DE LA TECHNOLOGIE, *L'utilisation des données biométriques à des fins de sécurité: questionnement sur les enjeux éthiques*, Study Document, (Sainte-Foy: 2005), p. 44.

204. R.S.Q., chapter P 39.1, 1993, c. 17, s. 14; 2006, c. 22, s. 115.

205. R.S.Q., chapter P-39.1, 1993, c. 17, s. 8.

transparent and in accordance with the fundamental values of democratic societies, individual consent is not necessarily required. It is essential, however, to bring together conditions that shed light on the process leading to the deployment of NSMT and to give opponents and critics all the necessary leeway so that they are allowed to voice their point of view. In addition, mechanisms should be implemented whereby groups or populations, who could be subject to surveillance within the context of very specific projects, could be consulted.

Information that must currently be provided by public and private organizations constitutes a minimum requirement. From an ethical perspective, and with regards to NSMT, it remains insufficient, and unhelpful to clear decision-making and public debate on the subject. Moreover, the Commission feels it necessary that the public be better informed, particularly, but not exclusively, with regards to the following points:

- The legal provisions surrounding the deployment of NSMT, the collection, use, disclosure and retention of personal information;
- The risks, disadvantages, advantages and potential benefits of the deployment of NSTM;
- Places and documents brought under surveillance;
- Means available to the public enabling their involvement in the deployment of NSMT, thereby allowing for an open and transparent process[206];
- Means available to the public to make its opinions known, including complaints against NSMT in general, or a NSMT deployment plan in particular.

Respect for the end purpose: Reaffirming the principle

Respect for the end purpose to which NSMT are deployed and the exploitation of all other possible uses are a source of tension. On one hand, respect for the stated end purpose is an important principle which tends to prevent diverted use and certain forms of abuse and excess. On the other hand, exploitation of all other possible uses of NSMT (including ends to which individuals have not given their consent) would probably allow for increased security.

This issue draws attention to the phenomenon of function creep, a potential risk that the Organization for Economic Co-operation and Development (OECD) defines as follows:

> *"Function creep" (also known as "purpose creep") is the term used to describe the expansion of a process or system, where data collected for one specific purpose is subsequently used for another unintended or unauthorised purpose.*
>
> *In privacy principle terms, we may think of function creep as a violation of the "finality" principles; the subsequent use, retention or disclosure of data without the consent of the individual and inconsistent with the purpose specification given at the time of data collection.*
>
> *As an example, we may think of a social service (welfare) system that requires a finger scan to enrol. Let us assume that undertakings were made at enrolment to the user that the finger scan is being collected solely for the purposes of guarding against 'double dipping' (ensuring that the user is not already registered for welfare). If the finger scan were subsequently used for another purpose (e.g. something not described in the initial purpose specification) then we have 'function creep'*[207].

Considering the examples brought to its attention, the Commission is concerned about the shifts it has observed and about those that could occur in the near future. Standards, procedures, practices, surveillance and monitoring methods implemented after the terrorist attacks have been progressively incorporated into the fight against petty crime, and eventually made their way into the business sector. Conversely, technologies such as RFID, whose applications are most often associated with retail businesses and inventory management, appear to be making their way into the realm of security. Moreover, considering how easily NSMT find a variety of applications and end purposes, a call for vigilance is deemed appropriate.

206. The Commission builds on works by the Information and Privacy Commissioner of Ontario on RFID. See Ann CAVOUKIAN, *Privacy Guidelines for RFID Information Systems (RFID Privacy Guidelines)*, Information and Privacy Commissioner/Ontario, June 2006, p. 2, available at <www.ipc.on.ca/images/Resources/up-rfidgdlines.pdf>.

207. ORGANISATION FOR ECONOMIC CO-OPERATION AND DEVELOPMENT, op. cit., p. 12.

Concerns pertaining to the normative framework

Section 65 of the Act respecting access to documents held by public bodies and the protection of personal information states that "A person who collects personal information verbally from the person to whom it relates on behalf of a public body must introduce himself and, when information is first collected and subsequently on request, inform that person […] of the purposes for which the information is collected[208]". Section 65.1, however, limits the scope of this section by stating the following:

A public body may, however, use such information for another purpose with the consent of the person to whom it relates, or without that consent, but only

1) *if the information is used for purposes consistent with the purposes for which it was collected;*
2) *if the information is clearly used for the benefit of the person to whom it relates; or*
3) *if the information is necessary for the application of an Act in Québec, whether or not the law explicitly provides for its use*[209].

The latter condition appears to open the door to a relatively open use of personal information, without regard for the end purposes for which this information was originally collected. Although the collection of personal information may well be restricted to the specified end purposes, subsequent use of this same information appears to easily slip by the rule of respect for the end purpose. From an ethical standpoint, the Commission believes that this is a source of concern with regards to the respect for the end purpose, and by the same token, respect for individual autonomy.

Concerns about the various NSMT

The proliferation of databases of all types raises fears about function creep. These databases can be pirated, sold or given access to, and there always remains a risk of unintended or inappropriate use by anyone who manages to gain access. A mobile medium, such as a card which can be carried around by its user, is less likely to be subject to function creep[210]. The information never finds its way into any database, and the user remains in complete control of his personal data.

In the case of video surveillance, function creep was vividly illustrated at Superbowl XXXV in Tampa Bay, in 2001. Conventional surveillance cameras were linked to a facial recognition program in order to compare facial images captured from the crowd with images of wanted criminals[211]. The Commission is concerned about this type of practice, considering the questionable reliability of facial recognition systems, which usually produce a high rate of false matches. To conduct an adequate ethical assessment of this type of function creep, one must be mindful of the intended spirit and purpose of this technology, as well as its risks and inconveniences. Individuals wrongfully identified as terrorists could suffer harmful consequences, and eventually find themselves in a position to unnecessarily have to defend and prove their innocence.

The Commission's concerns about function creep are somewhat exacerbated by the tendency for NSMT, along with developments in related technology, to become increasingly discreet. RFID tags are a good example. They can be used in a multitude of areas, and can transmit information from a remote location, even without the knowledge of their users. Tags incorporated into everyday objects could eventually contain all kinds of personal information that could be available to anyone equipped with the proper reading equipment.

Personal information found in tags could just as easily be used to assemble a consumer profile, confirm the identity of a passport holder or to read the medical file of an unconscious patient. The following example illustrates how function creep can have troubling and unexpected repercussions on security: A RFID tag implanted into a passport (well on its way to become standard practice) containing biometric data, as well as information

208. R.S.Q., chapter A-2.1, 1982, c. 30, s. 65; 1990, c. 57, s. 15; 2006, c. 22, s. 36.

209. R.S.Q., chapter A-2.1, 2006, c. 22, s.37.

210. PORTUGUESE DATA PROTECTION AUTHORITY, *Principles for the Use of Biometric Data in Controlling Access and Monitoring Hours Worked*, (Portugal: 26 February 2004), available at <http://www.cnpd.pt/english/bin/guidelines/Guidelines%20biometric%20(EN).HTM>; WORKING PARTY ON THE PROTECTION OF INDIVIDUALS WITH REGARD TO THE PROCESSING OF PERSONAL DATA, *Working Document on Biometrics*, (Brussels, Belgium: 1 August 2003), p. 6.

211. Philip E. AGRE , 'Your Face Is Not a Bar Code: Arguments against Automatic Face Recognition in Public', 10 September 2003, <http://polaris.gseis.ucla.edu/pagre/bar-code.html>.

pertaining to the holder's nationality, could be read by "unauthorized" scanners. The Commission addressed this phenomenon above in its discussion of covert tracking: An unauthorized person could read the tag's contents from a remote location without the tag holder's knowledge[212]. With respect to security, and considering terrorists' desire to target their attacks, this wrongful tracking could help terrorists "select" potential victims from a crowd based on their nationality, for instance[213].

Concerns about data retention

The storage period for data collected by NSMT constitutes an important element in the risk of function creep[214]. The principle is simple: Shorter data storage periods decrease the likelihood of function creep. Consequently, it is important to determine a data storage time frame before a surveillance system is implemented, and that it not exceed the normal storage period required to meet the intended purpose.

Finally, it must be noted that centralized storage of personal information also increases the risk that this information be used to assemble a detailed profile of an individual's habits. The question of end purpose compatibility raises the problem of the interoperability of various NSMT-related systems. Standardization required to allow interoperability could lead to databases being even more interconnected, which would increase the risk for abuse and excess resulting from function creep[215].

Concerns with the risk of discrimination and stigmatization

The analysis of personal information collected by NSMT involves a risk of discrimination and stigmatization. Given the nature of the personal information collected and the possibility of extracting information on ethnic origin, user health, consumer habits, or affiliation to political parties, questions regarding these issues must be raised. In the fight against terrorism, for instance, biometric data, images captured by surveillance cameras as well as information collected by RFID could lead to the targeting of certain groups who could become the object of discrimination and stigmatization[216]. In the case of video surveillance, studies show that system operators most often direct their attention to men of foreign origin[217]. Although surveillance systems are not implemented with the purposes of discrimination and stigmatization, the Commission feels that this type of outcome is as plausible as it is unacceptable.

* * *

NSMT do, nevertheless, offer considerable surveillance and risk assessment and management potential for security purposes, a point which should neither be ignored nor underestimated. Although some may see a threat to individual rights and freedoms in the growing popularity of surveillance methods, others with a more optimistic view will point to the crime and terrorism prevention potential of this technology.

On the whole, the risk of abuse and excess stemming from function creep, though possibly helpful in crime prevention or identifying criminals in certain cases, deserves full attention. By allowing the exploitation of all possible uses of NSMT in order to protect democracy and law and order against terrorism and other crimes, the Commission is concerned about compromising the very rights and liberties that constitute the founding principles of democracy. The Commission insists on the necessity to find an appropriate balance, and comes to the conclusion that democracy itself constitutes an ever-delicate balance between freedom and repression. NSMT can do much to help improve public safety, but it is not always necessary to resort to all of their possible applications.

212. WORKING PARTY ON THE PROTECTION OF INDIVIDUALS WITH REGARD TO THE PROCESSING OF PERSONAL DATA, *Working Document on Data Protection Issues related to RFID technology*, Brussels: 19 January 2005, p. 7. <http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2005/wp105_en.pdf>.

213. Ibid.

214. Terry HONESS and Elizabeth CHARMAN, *Closed Circuit Television in Public Places: Its Acceptability and Perceived Effectiveness*, Police Research Group, Crime prevention unit series: Paper nº 35, (London: Home Office Police Department), p. 15.

215. WORKING PARTY ON THE PROTECTION OF INDIVIDUALS WITH REGARD TO THE PROCESSING OF PERSONAL DATA, *Working Document on Data Protection issues Related to RFID Technology*, (Brussels: January 19, 2005), p. 6.

216. COMMISSION DE L'ÉTHIQUE DE LA SCIENCE ET DE LA TECHNOLOGIE, *L'utilisation des données biométriques à des fins de sécurité: questionnement sur les enjeux éthiques*, Document de réflexion, (Sainte-Foy: 2005), p. 44.

217. Gavin J.D. SMITH, 'Behind the Screens: Examining Constructions of Deviance and Informal Practices among CCTV Control Room Operators in the UK', *Surveillance & Society*, vol. 2, nº 2/3, p. 385-387; Ann Rudinow SÆTNAN, Heidi Mork LOMELL and Carsten WIECEK, 'Controlling CCTV in Public Spaces: Is Privacy the (Only) Issue? Reflections on Norwegian and Danish observations', *Surveillance & Society*, vol. 2, nº 2/3, p. 405-407.

Protection of personal information: Maintaining respect for privacy

The question of NSMT is often focused on a single issue: The protection of personal information. This is especially due to the fact that NSMT are essentially deployed to collect information (which is often personal). This issue, more than any other, concerns the values of privacy and security. If on one hand personal information reveals much about the private lives of individuals, it is nevertheless considered a valuable source of information allowing for improved security.

New information and communications technologies can both protect personal information and facilitate access to and sharing of the same information. Encryption technology, for instance, can be used to secure communication between two parties, but also promote a somewhat false sense of privacy, where communications could actually be intercepted[218]. In the current context, respect for privacy is an object of concern for another reason. The increasing number of databases created by organizations from both the public and private sector in itself deserves attention. These personal information collections are not unfamiliar to the risk society. As useful as they may be to organizations for purposes of security risk management, these databases that contain personal information on such a large scale create significant challenges with respect to the protection of confidentiality and uses that deviate from the original purpose.

The protection of personal information is almost systematically connected to privacy. It is true that information deemed personal opens a window into various aspects of our private lives. In fact, the issue of the protection of personal information requires an update of the concept of privacy. If the former is primarily a judicial concept, privacy, within the framework of this Position statement must be understood as a value.

Data collected by biometric systems, video surveillance and RFID almost systematically involve personal information. Consequently, the degree of respect for the privacy of those under surveillance will vary according to how it is used, stored and shared.

Each of the NSMT considered in this Position statement has its own way of dealing with personal information. Moreover, potential intrusion into private lives is different for each of them. For this reason, the Commission examined the links that connect the deployment of NSMT, privacy, and the protection of personal information by considering each NSMT separately.

Biometric data

The protection of personal information is inseparable from biometric systems since biometric measurements are considered personal information. The fact that certain biometric data constitute personal identifiers probably explains why biometric systems cause fear for the worst with regards to respect for individual privacy. Biometric data can be considered "revealing personal identifiers[219]" as they are intimately related to the individual from whom they were collected. The revealing nature of certain biometric identifiers is an object of concern: Biometric data contain more information than the simple reproduction of a fingerprint, for example. In fact, according to some experts, it is even possible to collect information on the health or mood of individuals simply by analyzing their fingerprints or retina[220]. People generally prefer that certain information in their possession, and as it pertains to them personally, remain confidential, or at least be treated as such[221].

In principle, access to personal information should only be given to those authorized to do so. A problem can arise when an individual exercises his right to access colligated information or to correct this information (sections 83 and 89 of the Act respecting access to documents

218. UNESCO, op. cit., p. 14.

219. COMMISSION D'ACCÈS À L'INFORMATION DU QUÉBEC, *La biométrie au Québec: les enjeux*, Analytical Document, July 2002, p. 25.

220. INSTITUTE FOR PROSPECTIVE TECHNOLOGICAL STUDIES, *Security and Privacy for the Citizen in the Post-September 11Digital Age: A Prospective Overview*, Report to the European Parliament Committee on Citizens Freedoms and Rights, Justice and Home Affaires, (European Commission, July 2003), pp. 50-54.

221. Ann CAVOUKIAN, *Biometrics and Policing: Comments from a Privacy Perspective*, Information and Privacy Commissioner/Ontario, August 1999, p. 10.

held by public bodies and the protection of personal information, sections 27 and 28 of the Act respecting the protection of personal information in the private sector and section 40 of the Civil Code[222]), due to the raw data digitization process that renders this data virtually indecipherable[223]. It thus becomes almost impossible to verify the authenticity of a "signature", which anyone can do when, for instance, they want to make sure their credit history is up to date and accurate.

According to industry experts, biometric technology is not intrusive in itself, and can be effective in helping reduce invasion of privacy[224]. These experts claim that neither privacy nor security need to be compromised to guarantee the other, and that both can benefit from transparent and legitimate use of a well-conceived biometric system.

The *Commission d'accès à l'information* defines the links between security and privacy with regards to the use of biometric data:

> *Although most biometric techniques are very effective in areas of security, they are less than stellar with regards to user privacy and data protection. It is important to make a clear distinction between the concept of security and that of privacy and personal information. Security mechanisms are often intrusive to the privacy of their users, as recently demonstrated by the Commission d'accès à l'information's Position statement on government public key infrastructure. This invasion of privacy involves the collection of additional information, the processing of this information, and the possibility of tracing, tracking and profiling*[225].

Repercussions on privacy are not a direct cause of the technology itself, but rather the way in which it is used. In the case of a personal authentication system (to find out if a person is who he claims to be), decentralized data storage is generally sufficient. But in the case of personal identification (to find out who this person is), particularly in legal cases, the process involves scanning centralized data from one or more databases. Some security experts agree that centralized databases represent a risk of their own[226], and with regards to biometric data stored on mobile media, potential theft or data capture without user knowledge must be considered[227].

It is important to note that biometric systems use computer systems set up individually or via a network. When stored in a centralized memory as opposed to a hard drive or tag, biometric data "travels" and can be linked to other information found in other databases that contain other types of information related to the same individuals. As more and more information concerning an individual is matched up, a more complete profile of this person begins to emerge. To consider another possibility, as the information "expands", and the database grows, the hungrier computer pirates will become in their attempts to maliciously and financially take advantage of the "many weaknesses found in these networks, software and databases[228]".

Fortunately, as noted by the CAI, Québec law prohibits the sharing of personal information collected by organizations, except under circumstances, and encourages a cloistering of this information in order to protect privacy[229]. Nevertheless, in a context where information system centralization and integration becomes economically desirable, and with access to information by an increasing number of people, comes a growing risk that a state would seek to use this goldmine of information for a variety of purposes, whether or not for the benefit of society as a whole, or for certain more vulnerable segments of society.

Video surveillance

Due to its remote and invisible nature, video surveillance can represent a threat to privacy. Technology readily

222. COMMISSION D'ACCÈS À L'INFORMATION DU QUÉBEC, *La biométrie au Québec: les enjeux*, Analytical Document, July 2002, p. 37.
223. OFFICE PARLEMENTAIRE D'ÉVALUATION DES CHOIX SCIENTIFIQUES ET TECHNOLOGIQUES, op. cit., 2e partie, pp. 21-22.
224. CITIZENSHIP AND IMMIGRATION CANADA, *Biometrics: Implications and Applications for Citizens and Immigration*, Background Paper, Forum held October 7 & 8 2003, Ottawa, Canada, p. 19.
225. COMMISSION D'ACCÈS À L'INFORMATION DU QUÉBEC, *La biométrie au Québec: les enjeux*, Analytical Document, July 2002, p. 23.
226. Ibid., p. 30.
227. Ibid., p. 33.
228. Ibid., p. 30.
229. Ibid., p. 26.

allows for the filming of people without their knowledge, in both public and private areas. Therefore, individuals must realize that they do not enjoy the same levels of intimacy in public places as they do in their homes, for example. It would be an exaggeration, however, to expect individuals to completely renounce any right to privacy in public places. Everyone is entitled to expect to be able to move about in public without being the object of constant surveillance. Respect for privacy also applies to public places.

Radio frequency identification

Europe has established itself as a pioneer with respect to issues pertaining to the protection of personal information and privacy raised by RFID. Working Party 29 briefly summarizes this issue as follows:

Privacy and the Protection of Personal Information With Regards to RFID: A Brief Summary by Working Party 29

While the advantages related to the use of RFID technology seem obvious, the widespread deployment of the technology does not come without its potential drawbacks. On the data protection front, Working Party 29 ("Working Party 29") is concerned about the possibility for some applications of RFID technology to violate human dignity as well as data protection rights. In particular, concerns arise about the possibility of businesses and governments to use RFID technology to pry into the privacy sphere of individuals.

The ability to surreptitiously collect a variety of data all related to the same person; track individuals as they walk in public places (airports, train stations, stores); enhance profiles through the monitoring of consumer behaviour in stores; read the details of clothes and accessories worn and medicines carried by customers are all examples of uses of RFID technology that give rise to privacy concerns. The problem is aggravated by the fact that, due to its relative low cost, this technology will not only be available to major actors but also to smaller players and individual citizens[230].

Also significant is the analysis offered by a Commissioner of the *Commission nationale de l'informatique et des libertés (CNIL)* concerning the traps that "attempt to downplay the risks to privacy and protection of personal data generated by this technology[231]" who believes that the issue of privacy may well end up being ignored due to the very characteristics of RFID:

- *(apparent) lack information significance;*
- *priority given to objects [in appearance, always vis-a-vis people;*
- *Concept of globalization [technological standardisation based on the American concept of "privacy" without consideration for European privacy protection principles];*
- *The risk of personal "non-vigilance" [presence and invisible action]*[232].

Just as with video surveillance, radio frequency identification (RFID) could become a surreptitious means of surveillance and used to trace and track individuals. For this reason, the Commission's comments with regards to video surveillance apply equally to RFID. The Commission wishes to point out, however, that the nature of the collected information is different. With video surveillance, personal information is collected in the form of images, possibly including faces. In the case of RFID, crucial personal information is likely to be collected: Credit card information, health, identity, nationality, etc. The nature of this information presents a heightened risk to individual privacy.

The main current use of RFID is found in the tags containing biometric data incorporated into passports. The purpose here is to deter counterfeit and identity theft. It must be recognized, however, that current systems do not protect this information through an encryption process. It has been shown that with rudimentary equipment, RFID tags are easily duplicated and inserted into a forged passport that is undistinguishable from the original[233]. The lack of encryption would therefore allow the information to be intercepted as it is scanned. In other words, the tag could be read while in transit by

230. WORKING PARTY ON THE PROTECTION OF INDIVIDUALS WITH REGARD TO THE PROCESSING OF PERSONAL DATA, *Working Document on Data Protection issues Related to RFID Technology*, (Brussels: January 19, 2005), p. 2, available at <http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2005/wp105_en.pdf>.

231. COMMISSION NATIONALE DE L'INFORMATIQUE ET DES LIBERTÉS, 'La radio-identification', *cnil.fr*, 30 June 2006. <http://www.cnil.fr/index.php?id=1063>.

232. Ibid.

233. Kim ZETTER, op. cit.

an unauthorized entity. Finally, identity documents that can be read at different "points of service" could allow users to be tracked.

From there, three types of risk threaten privacy[234]. The first pertains to the risks associated with the collection of information that could directly or indirectly involve personal information. Obviously, this type of risk is not limited to RFID. The second type of risk occurs when personal information is stored on RFID tags, such as passports that include a scanned fingerprint, for instance. Finally, the third type of risk is raised when RIFD allows for tracing and tracking of individuals. In fact, if tags contain personal information, any reading of these tags, whether authorized or not, can confirm the presence of an identifiable individual at that specific moment.

In an attempt to thwart these risks, a consensus has emerged around the use of privacy-friendly technologies (or privacy enhancing technologies) for use in RFID To this effect, the Information and Privacy Commissioner of Ontario has stated that privacy concerns should be central to the development of RFID, and that these issues be addressed early in the design stages[235]. Since new passports issued by most members of the European Union as well as those currently issued to American citizens contain a RIFD tag, and given the interest the Government of Canada has shown in incorporating biometric data into identity documents, the Commission believes a ruling will soon be needed on how to manage the introduction of this technology into identity documents. Moreover, the European and American experiences demonstrate the importance of adequately protecting personal information if the goal of securing identity documents is to be achieved. For its part, and considering the substantial risks to privacy and the protection of personal information, the Commission believes it important that the Government of Québec work in concert with the appropriate Canadian government authorities so that, in the event that RFID tags would work their way into Canadian identity documents, that these tags feature an encryption process to secure this data, and in so doing, provide better privacy and personal information protection.

Automatic data processing: A practice that raises concerns

In its study document on biometrics, the Commission has also raised the issue of automatic data processing, a practice which is not above raising serious concerns, and that is applicable to all three NSMT described in this Position statement:

> *On this subject, and also concerning other aspects of information conveyed by biometric data, it must be recognized that decisions concerning individuals could be taken automatically by computerized systems solely on the basis of the available information. Such decisions, taken without the individual's knowledge, and based on information used out of context and facts that are at times incomplete, inaccurate, irrelevant or useless, could be harmful to that individual*[236].

It would be unacceptable for decision-making based on automatic data processing to become common practice in surveillance and identity monitoring. Dehumanization in security-related decisions must be avoided. Once again, it appears that a balance must be struck between man and machine with regards to surveillance and data processing. On one hand, the more surveillance systems are managed by people, the more we can expect their life experiences to occasionally influence their decisions. But let us not be deluded: No one can completely set aside their personal views and opinions in the exercise of their work. Moreover, if computerized and automated data processing can reduce the prejudicial influence of surveillance system operators, it remains nonetheless a concern to think that potentially harmful decisions could be taken on the basis of this processing, without anyone having placed this information in its proper context.

Cross-border transfer of personal information

Finally, one must question whether the level of protection of personal information is the same from one country to another, and whether the transfer of this information from a country with high levels of protection towards

234. EUROPEAN COMMISSION, *RFID Security, Data Protection and Privacy, Health and Safety Issues*, Policy Framework Paper, 11 May 2006, p. 10. <http://www.rfidconsultation.eu/41/38/264.html>.

235. Ann CAVOUKIAN, *Privacy Guidelines for RFID Information Systems (RFID Privacy Guidelines)*, Information and Privacy Commissioner/Ontario, juin 2006, p. 2. <http://www.ipc.on.ca/images/Resources/up-1rfidgdlines.pdf>.

236. Commission de l'éthique de la science et de la technologie, *L'utilisation des données biométriques à des fins de sécurité: questionnement sur les enjeux éthiques*, (Sainte-Foy: 2005), p. 44.

a country with less to offer is acceptable. Consumers are already conducting transactions on the Internet with foreign companies which store their personal information, without any knowledge as to how this information is to be protected. Yet, consumers remain free to abstain from participating in such transactions. But with information obtained through NSMT, individuals are not always aware that their personal information will be stored. Obviously, this raises questions about individuals and their control over the fate of their personal data.

* * *

This Position statement brings to light questions to which the Commission is not in a position to provide answers and to which it cannot ensure a follow-up. The Commission does, however, feel that several actions must be taken to find solutions and that the governmental actors who can accomplish them can be readily identified.

Considering that the Minister responsible for Canadian Intergovernmental Affairs, Aboriginal Affairs, Francophones within Canada, the Reform of Democratic Institutions and Access to Information has the mandate to advise the Government by providing Position statements with regards to access to information and the protection of personal information, particularly during the tabling of bills or the development of information systems, and that the *Commission d'accès à l'information* may be consulted for these purposes;

Considering that the *Commission d'accès à l'information* is responsible for ensuring compliance with, and the promotion of, access to documents and the protection of personal information, and can determine the conditions applicable to a personal information file to which a public body must comply;

Considering that the *Commission d'accès à l'information* can also, after due investigation relative to the collection, retention, disclosure or use of personal information by a person in the course of carrying on an enterprise, and after having given this individual an opportunity to present his observations, recommend or order this person to apply any and all corrective measures required to ensure the protection of personal information;

And considering that the *Commission des droits de la personne et des droits de la jeunesse du Québec* is mandated to:

- Design and implement an information and educational program on human rights as well as the protection of children's rights;
- Direct and encourage research and publications on fundamental rights and freedoms and on children's rights;
- Receive suggestions, recommendations and requests regarding human rights and freedoms, by holding public hearings as needed, and to submit appropriate recommendations to the Government;
- Cooperate with any and all organizations devoted to the promotion of human rights and freedoms, both within and outside of Québec,

The Commission recommends to the Minister responsible for Canadian Intergovernmental Affairs, Aboriginal Affairs, Francophones within Canada, the Reform of Democratic Institutions and Access to Information, the *Commission d'accès à l'information* and the *Commission des droits de la personne et des droits de la jeunesse du Québec* to work together in order to implement the following actions:

1. **Promote a dialogue among citizens, the Government and the industry towards the adoption of guidelines regarding the use of these technologies that take into account the ethical concerns with respect to fundamental democratic values.**
2. **Through a consultative approach, advise the Government with regards to its NSMT deployment projects, particularly in areas which raise ethical issues and according to the criteria of relevance, effectiveness and reliability.**
3. **Organize a public consultation process (based on the model developed by the *Commissaire à la santé et au bien-être*) that would highlight ethical issues.**
4. **Make the results of this consultation publicly available in order to sensitize the general population as to the ethical issues associated with NSMT.**
5. **Inform the general population as to the legal provisions surrounding the deployment of NSMT and its consequences on the values of autonomy, freedom, security and privacy, and the means available to the public to participate in the decision-making, implementation and follow-up processes involved.**
6. **Implement a compensation and correction mechanism for cases where the use of NSMT is prejudicial to individuals by wrongfully associating them with illicit activities.**

Conclusion

Aiming for a proper balance among fundamental democratic values is a tall order, especially when there is conflict among these values. The deployment of NSMT clearly illustrates this issue. The consideration of contextual elements such as the prevalence of a renewed concern for security, feelings of insecurity, risk and surveillance has allowed for a broader look at the ethics involved.

The Commission has insisted on explicitly defining the ethical framework from which it conducted its analysis. A discussion of the values at stake and the ethical issues involved precedes a detailed presentation of the various NSMT. Moreover, throughout the entire process leading to the publication of this document, the Commission has come to an awareness of the extent to which the boundaries that separate public and private spaces are blurred, and continue to become increasingly so. This observation has a direct impact on the ethics involved as the value of privacy is increasingly subject to debate, if not altogether called into question. The Commission was further compelled to present the various normative instruments currently in place, in Québec, Canada, and at the international level. In addition, special attention was given to the legal definition of personal information, a concept at the center of this analysis.

The Commission focused its ethical look on three technologies. Biometric systems, video surveillance, and radio frequency identification (RFID), each receiving separate treatment in order to better familiarize the reader with these technologies. Providing better knowledge and understanding of the end purposes, current applications, their method of operation, benefits, drawbacks as well as market tendencies and public interest regarding these technologies was deemed necessary to a broader and deeper understanding of the issues. For this reason, the Commission has dedicated an entire chapter to a presentation and analysis of NSMT. Experts reveal the increasing presence of these technologies in our daily lives. The security market is in full growth, and in response to an evident public need. As with other emerging technologies, NSMT offer great promise and hope in both the improvement of security and user-friendliness. These technologies, however, are not without their drawbacks.

The Commission has focused on six ethical issues raised by NSTM. No one particular value was given disproportionate importance over any other, the purpose being to seek a proper balance.

To begin with, the Commission focused on the assessment of the relevance, efficiency and reliability of NSMT. In order be legitimately deployed, NSMT must be relevant, effective and reliable. Having acknowledged that NSMT are not yet in a position to fulfill all of their promises, the Commission calls for caution. The deployment of technology perceived as reliable that would contribute to promoting a false sense of security among the public would be unacceptable.

With regards to the issue of the proportionality of response to insecurity, the Commission expressed its concerns over the scale a deployment of NSMT could reach in response to an insatiable demand for more security. Implementation of NSMT must seek to achieve an acceptable level of security, nothing more. Since each NSMT deployment project is different in many regards, the assessment of the relationship between technical reliability, proportionality of response to insecurity and the degree of invasion of privacy involved must be individually redone for each and every project. A deployment that successfully meets an acceptable level of security must involve a dialogue between decision-makers in both the public and private sectors. Certainly, implementation of surveillance methods that are too intrusive, or collection of personal information that is not necessary to the end purpose are unacceptable, regardless of the project. The Commission, therefore, urges political and private decision-makers to conduct a

careful and lucid assessment of NSMT needs for security purposes. Furthermore, considering that suppliers and fitters are the ones to determine the proportionality of technological means in response to insecurity, and are the first to be confronted with the ethical issues mentioned by the Commission, it is necessary that they be sensitized to these issues in order that any NSMT deployment be conducted in accordance with cherished values. The Commission recommends that training provided by the *Bureau de la sécurité privée* to representatives of licensed agencies include a compulsory ethics component based on the ethical issues raised in this Position statement, and that the Government, in compliance with the Private Security Act, adopt the necessary regulations so that the training required for the deliverance of an agent licence also include an ethics component.

With regards to social acceptability, any consultation process on NSMT must place a high premium on public participation, and above all, seek informed and enlightened opinions.

By the very nature of NSMT, it is very difficult, if not impossible, to obtain free and informed individual consent of individuals placed under surveillance. The issue of consent thus raises many challenges. In addition, the Commission draws attention to the limitations of the legal provisions that govern the collection and disclosure of personal information. The public must be better informed about the legal provisions surrounding the collection, use, disclosure and retention of personal information, as well as the risks, drawbacks, advantages and potential benefits of NSMT deployment, the places and documents brought under surveillance and the means available to the public enabling their involvement in the deployment of NSMT, thereby allowing for an open, transparent and changeable implementation process.

As for respect for end purpose, the tension that exists between the declared end purposes and the exploitation of all possible uses of a NSMT deployment is at the heart of another ethical issue. Moreover, factors such as the storage period of personal information can influence the risk of excess and abuse, such as discrimination and stigmatization. The Commission acknowledges the fact that NSMT can do much to help improve public safety, but believes that it is not always necessary to resort to all of their possible applications to ensure an acceptable level of security.

The protection of personal information constitutes a way to update the value of privacy. As each NSMT establishes its own singular relationship with this issue, biometric systems, video surveillance and radio frequency identification are all treated separately. With regards to biometric systems, the Commission expresses reservations about the disclosure of personal information of a biometric nature, and maintains a preference for systems where users maintain maximum control over their personal information. It bears repeating that biometric data are identifiers that are intimately associated with an individual (since the probability that two people share the same biometric feature is little to none) and can reveal more than the individual's identity. The Commission also expresses concern over the intrusive aspect of video surveillance with respect to privacy. Finally, the Commission draws attention to the fact that data stored in a RFID tag constitute personal information. In addition, the inclusion of these tags in identity documents, for instance, raises the possibility of tracking the movements of individuals in time and space. More troubling yet, passports equipped with these tags have proven to be easy to falsify. Considering the substantial risks to privacy and the protection of personal information involved, the Commission believes it important that the Government of Québec work in concert with the appropriate Canadian government authorities so that, in the event that RFID tags would work their way into Canadian identity documents, that these tags feature an encryption process to secure this data, and in so doing, provide better privacy and personal information protection.

In addition, the Commission cautions against standardized covertness in automated data processing. This troubling practice is likely to cause harm to innocent people since decisions concerning them can be made out of context by a single automated processing action.

The protection of personal information, in an era where this information travels without regard for borders, is a major issue for anyone who wishes to maintain control over the fate of their personal information.

Generally speaking, the Commission is not concerned about the emergence of a totalitarian state so much as the advent of mass surveillance by the masses, in other words, that several organizations and individuals begin to privately conduct surveillance for security purposes.

Although the Commission has treated biometric systems, video surveillance and radio frequency identification separately throughout this Position statement, this choice in methodology does not reflect the increasing tendency for the various surveillance and monitoring technologies to converge. Biometric facial recognition software, the inclusion of biometric data in RFID tags and other hybrids currently in use offer a glimpse into the future of surveillance systems. The effects, both beneficial and detrimental, can only multiply.

Given the considerable amount of work that yet needs to be done in order to properly manage the NSMT deployment, and that several required actions extend beyond the Commission's mandate, a recommendation is issued to government authorities who are strategically positioned to achieve these goals.

The groundswell of insecurity, obsession for the elimination of risk, security, as well as implementation of intrusive surveillance methods, are toxic to democracy. NSMT deployment that is done in accordance with fundamental democratic values can help deter these threats. However, a fair balance must be struck so that the use of this surveillance technology does not undermine the very basis of the democratic ideal: To ensure an acceptable degree of security without violating the values of autonomy, freedom, privacy and transparency. With this Position statement, the Commission hopes to have charted a course for dialogue on the ethical issues associated with NSMT among all concerned actors. Its thinking, opinions and recommendations constitute its contributions to a broader public debate it hopes will take place.

Glossary[237]

Cybersurveillance – Set of surveillance and monitoring tools applied to people or processes, tied to new information technologies and digital communication networks.

Data Mining – Data research and analysis technique which allows one to extract hidden trends or correlations from large data sets, or to identify strategic information or provide knowledge discovery based on statistical methods.

Digitization – Use of a scanner to automatically digitize analogue information (text or image).

DNA – High-weight macromolecule made of nucleotide polymers the sugar of which is 2-deoxyribose. DNA takes the shape of two long strands entwined in a double helix and is at the source of the genome of most living organisms.

Encryption – The process of transforming a clear text into one that is unreadable and useless to anyone who does not possess the key to bring the text back to its original state.

Thermography (Thermal imaging) – Process by which it is possible to view and record the thermal radiation organisms emit through their skin.

Victimization – Attitude by which a subject poses as a victim to consciously or unconsciously provoke feelings of pity or guilt in others and protect oneself against accusation or punishment while indirectly demanding satisfaction of one's material and affective needs.

237. Except for 'cybersurveillance', the definitions have been taken and translated from the *Grand dictionnaire terminologique*. The definition of 'cybersurveillance' is taken from Murielle CAHEN, 'Le rôle de l'administrateur réseau dans la cybersurveillance', <http://www.netalya.com/fr/article2.asp?CLE=162>.

Bibliography*

'Does Facial Recognition Measure Up? Canada's Passport Office Answers the Question', *IIJ@WORK*. Summer 2004.

'Canadians and Americans Support Biometric Technology in Passports and Drivers' Licences: Survey', Press release. Toronto, August 2, 2005.

'Research: World CCTV Market to Grow 37 Percent by 2009', *SecurityInfoWatch.com*, 14 July 2006. http://www.securityinfowatch.com/online/Research--Studies-and-Whitepapers/8702SIW321.

'New York Times-CBS News Survey', 17-21 August 2006.

Agre, Philip E. *Your Face Is Not a Bar Code: Arguments against Automatic Face Recognition in Public*, 10 September 2003. http://polaris.gseis.ucla.edu/pagre/bar-code.html.

Association sur l'accès et la protection de l'information. *L'utilisation de caméras de surveillance par des organismes publics dans des lieux publics*, Mémoire presented to the Commission d'accès à l'information during its public consultation, September 2003.

Beck, Ulrich. *Risk Society: Towards a New Modernity*. Sage, 1992.

Bureau d'audiences publiques sur l'environnement. *Le projet de la Régie intermunicipale de gestion des déchets sur l'île de Montréal*, Rapport d'enquête et d'audience publique, 1993.

Canadian Security Association, *Pour un monde en toute sécurité*, Memoir presented to the Commission d'accès à l'information, 2 September 2003.

Cap Gemini Ernst & Young. *RFID and Consumers. Understanding Their Mindset, A U.S. Study Examining Consumer Awareness and Perceptions of Radio Frequency Identification Technology*, Executive Summary. 13 January 2004. http://www.rfidconsultation.eu/docs/ficheiros/CPRD_RFID_mindset_ES.pdf.

Cavoukian, Ann. *Biometrics and Policing: Comments from a Privacy Perspective*, Information and Privacy Commissioner/Ontario, August 1999.

Cavoukian, Ann. *Guidelines for Using Video Surveillance Cameras in Public Spaces*, Information and Privacy Commissioner/Ontario, October 2001. www.ipc.on.ca/images/Resources/video-e.pdf.

Cavoukian, Ann. *Privacy Guidelines for RFID Information Systems (RFID Privacy Guidelines)*, Information and Privacy Commissioner/Ontario, June 2006, www.ipc.on.ca/images/Resources/up-rfidgdlines.pdf.

Citizenship and Immigration Canada, *Biometrics: Implications and Applications for Citizens and Immigration*, Background Paper, Forum held October 7 & 8 2003, Ottawa, Canada.

Citizenship and Immigration Canada, *Biometrics: Implications and Applications for Citizens and Immigration*, Report on a Forum held October 7 & 8 2003, Ottawa, Canada.

* Except where mentioned, all Internet addresses were accessible on March 3rd, 2008, either directly or through the archives of certain sites.

Clark, Campbell. 'Canadians Want Strict Security: Poll', *GlobeandMail.com*, 11 August 2005. http://www.theglobeandmail.com/servlet/story/RTGAM.20050811.wxsecurity11/BNStory/National/.

Comité consultatif national d'éthique pour les sciences de la vie et de la santé. *Biométrie, données identifiantes et droits de l'homme*, Position statement nº 98, 26 April 2007. www.comite-ethique.fr/docs/fr/avis098.pdf.

Commission d'accès à l'information du Québec. *La biométrie au Québec: Les enjeux*, Analytical Document, July 2002. http://www.cai.gouv.qc.ca/06_documentation/01_pdf/biom_enj.pdf.

Commission d'accès à l'information du Québec, *Biometrics in Québec: Application Principles, Making an Informed Choice*. July 2002. http://www.cai.gouv.qc.ca/home_00_portail/01_pdf/biometrics.pdf.

Commission d'accès à l'information du Québec. *Radiofrequency identification technology (RFID): Is there reason to mistrust it?*, Analytical Document, May 2006. http://www.cai.gouv.qc.ca/06_documentation/01_pdf/RFID_en.pdf.

Commission de l'éthique de la science et de la technologie. *Pour une gestion éthique des OGM*. Sainte-Foy: 2003.

Commission de l'éthique de la science et de la technologie. *L'utilisation des données biométriques à des fins de sécurité: questionnement sur les enjeux éthiques*. Study Document. Sainte-Foy: 2005.

Commission de l'éthique de la science et de la technologie. *L'utilisation des données biométriques à des fins de sécurité: questionnement sur les enjeux éthiques*, Study Document. Sainte-Foy: 2005.

Commission nationale de l'informatique et des libertés. 'La radio-identification', *cnil.fr.* 30 June 2006. http://www.cnil.fr/index.php?id=1063.

Compas. *Terror after London*, BDO Dunwoody/Chamber Weekly CEO/Business Leader Poll by Compas in the Financial Post. 18 July 2005.

Dandeker, Christopher. *Surveillance, Power and Modernity*. New York: St. Martin's Press, 1990.

Deleurence, Guillaume. 'Le passeport se convertit à l'électronique, avant la biométrie', *01net.com*. 28 August 2006. http://www.01net.com/editorial/324183/societe/le-passeport-se-convertit-a-l-electronique-avant-la-biometrie/.

Dionne, Bernard and Èvelyne Racette. 'La biométrie: présentation à la Commission de l'éthique de la science et de la technologie', March 2004 [manuscript].

Duce, Helen. *Executive Briefing, Public Policy: Understanding Public Opinion*, Auto-ID Centre. 1 February 2003. http://www.autoidlabs.org/single-view/dir/article/6/199/page.html.

Electronic Privacy Information Center. 'Radio Frequency Identification (RFID) Systems', *epic.org*. 13 January 2006. http://www.epic.org/privacy/rfid/.

Ericson, Richard V. and Kevin D. Haggerty. *Policing the Risk Society*. Toronto: University of Toronto Press, 1997.

European Commission, *Data Protection in the European Union: Dialogue with Citizens and Business*. Belgium: 2000.

European Commission. *RFID Security, Data Protection and Privacy, Health and Safety Issues*, Policy Framework Paper. 11 May 2006. http://www.rfidconsultation.eu/41/38/264.html.

European Commission. *Your Voice on RFID. Background document for public consultation on Radio Frequency Identification (RFID) – Summary of five workshops*. July 2006. http://www.rfidconsultation.eu/docs/ficheiros/Your_voice_on_RFID.pdf.

European Parliament and the Council of the European Union, 'Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data', *Official Journal*, L 281 , 23/11/1995 P. 0031 – 0050. http://europa.eu.int/eur-lex/lex/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:EN:HTML.

Ewald, François. *L'État providence*. Paris: Bernard Grasset, 1986.

Fédération des travailleurs et travailleuses du Québec. *Mémoire de la Fédération des travailleurs et travailleuses du Québec présenté à la Commission d'accès à l'information du Québec sur l'utilisation de caméras de surveillance par des organismes publics dans les lieux publics*. Montréal, 22 September 2003. http://www.ftq.qc.ca/modules/documents/index.php?id=5&langue=fr.

Ferry, Luc. 'La nouvelle société du risque', in *Liberté, risque & responsabilité: nouveaux repères à l'heure de la mondialisation et du terrorisme international*. Paris: Institut français des relations internationales, 2001.

Flaherty, David H. *Protecting Privacy in Surveillance Societies*. Chapel Hill: University of North Carolina Press, 1989.

Foster, Kenneth R. and Jan Jaeger, 'RFID Inside. The Murky Ethics of Implanted Chips', *IEEE Spectrum*. March 2007. http://pages.cs.wisc.edu/~markhill/cs252/Spring2007/handouts/spectrum07_rfid_ethics.pdf.

Freedom of Information and Protection of Privacy. *Guide to Using Surveillance Cameras in Public Areas*, Government of Alberta, June 2004. http://foip.gov.ab.ca/resources/publications/pdf/SurveillanceGuide.pdf.

Hempel, Leon and Eric Töpfer. *CCTV in Europe, Final Report*, Working Paper No.15, August 2004. http://www.urbaneye.net/results/ue_wp15.pdf.

Honess, Terry and Elizabeth Charman. *Closed Circuit Television in Public Places: Its Acceptability and Perceived Effectiveness*, Police Research Group, Crime Prevention Unit Series: Paper No. 35. London: Home Office Police Department.

IDTechEx. *RFID Forecast, Players & Opportunities 2006-2016*, October 2006.

Industry Canada. *Canadian Security Industry Hotspots*. http://www.ic.gc.ca/epic/site/ict_c-g_tic.nsf/en/tk00526e.html.

Institute for Prospective Technological Studies. *Biometrics at the Frontiers: Assessing the Impact on Society*, Technical Report Series. 2005, pp. 39-40.

Institute for Prospective Technological Studies, *Security and Privacy for the Citizen in the Post-September 11Digital Age: A Prospective Overview*, Report to the European Parliament Committee on Citizens Freedoms and Rights, Justice and Home Affaires. European Commission, July 2003.

International Biometric Group, *Biometrics Market and Industry Report 2007-2012*.

International Biometric Industry Association. *IBIA Statement of Principles and Code of Ethics*, 23 October 2000. http://www.ibia.org/aboutibia/ethics.asp.

Jonas, Hans. *Le principe responsabilité: une éthique pour la civilisation technologique*. Paris: Éditions du Cerf, 1990.

Lamalice, Olivier. *Public opinion, incarceration and the American penal system: The influence of the political elite and the media* (in French), document d'appoint préparé pour le ministère de la Sécurité publique. http://www.msp.gouv.qc.ca./reinsertion/publicat/severite_penale/severite_penale_partie1.pdf.

Laporte, Michel. *Bilan*, Public consultation: Use of surveillance cameras by public bodies in public places. Commission d'accès à l'information, April 2004. http://www.cai.gouv.qc.ca/06_documentation/01_pdf/bilan.pdf.

Le Breton, David. *Sociologie du risqué*. Paris: Presses Universitaires de France, 1995.

Lee, Murray. 'Governing "Fear of Crime" ', in Richard Hil and Gordon Tait (dir.) *Hard Lessons*. Ashgate: Hants, 2004.

Léger Marketing. *Safety in Canada According to Canadians*, Report. 2002.

Léger Marketing. *Feelings of Safety Among Canadians*, January 2003.

Léger Marketing. *Étude sur le sentiment de sécurité des Montréalais*, March 2004.

Léger Marketing. *Are Other Terrorist Attacks Imminent? September 11 from the Point of View of Canadians: 5 Years Later – Part 1*. August 2006.

Léger Marketing. *Montréal une ville sécuritaire, attrayante mais malpropre*, February 2007.

London School of Economics & Political Science. *The Identity Project. An Assessment of the UK Identity Cards Bill & Its Implications*. Department of Information Systems, 27 June 2005.

Lyon, David. *The Electronic Eye*. Minneapolis: University of Minnesota Press, 1994.

Lyon, David. *Surveillance Society: Monitoring Everyday Life*. Buckingham: Open University Press, 2001.

Masson, Isabelle. "Sécurité", in Alex Macleod, Évelyne Dufault et F. Guillaume Dufour (dir.), *Relations internationales: théories et concepts*. Montréal: Athéna éditions, 2004.

Ministère de la Sécurité publique du Québec, *Partners in Crime Prevention: For a Safer Québec*, Report of the Task Force on Crime Prevention. 1993. http://www.msp.gouv.qc.ca/prevention/prevention_en.asp?txtSection=publicat&txtCategorie=table_ronde.

Ministère de la Sécurité publique du Québec. *2005-2008 Strategic Plan*, Gouvernement du Québec, 2005.

Norris, Clive and Gary Armstrong. *The Maximum Surveillance Society: The Rise of CCTV*. Oxford: Berg, 1999.

Office of the Information & Privacy Commissioner for British Columbia. *Public Surveillance System Privacy Guidelines*. 26 January 2001. http://www.oipcbc.org/advice/VID-SURV(2006).pdf.

Office of the Privacy Commissioner of Canada, *OPC Guidelines for the Use of Video Surveillance of Public Places by Police and Law Enforcement Authorities*, March 2006. http://www.privcom.gc.ca/information/guide/vs_060301_e.asp.

Office of the Saskatchewan Information and Privacy Commissioner. *Guidelines for Video Surveillance by Saskatchewan Public Bodies*. 24 June 2004. www.oipc.sk.ca/webdocs/VideoSurveillance.pdf.

Office parlementaire d'évaluation des choix scientifiques et technologiques. *Les méthodes scientifiques d'identification des personnes à partir de données biométriques et les techniques de mise en œuvre*, Report presented to the Senate by Christian Cabal. France: Assemblée nationale, June 2003.

Organisation for Economic Co-operation and Development (OECD). *Biometric-based Technologies*, Working Party on Information Security and Privacy, Directorate for Science, Technology and Industry, Committee for Information, Computer and Communications Policy. Paris: 28 April 2004.

Peretti-Watel, Patrick. *Sociologie du risqué*. Paris: Armand-Colin, 2000.

Portuguese Data Protection Authority. *Principles for the Use of Biometric Data in Controlling Access and Monitoring Hours Worked*. Portugal: 26 February 2004. http://www.cnpd.pt/english/bin/guidelines/Guidelines%20biometric%20(EN).HTM.

Privacy International. *Overview of Privacy*, 29 October 2006. http://www.privacyinternational.org/article.shtml?cmd[347]=x-347-543673&als[theme]=Privacy%20and%20Human%20Rights.

Robin, Corey. *Fear. The History of a Political Idea*. New York: Oxford University Press, 2004.

Rodotà, Stefano. 'Privée (Protection de la vie)', in Gilbert Hottois and Jean-Noël Missa (dir.), *Nouvelle encyclopédie de bioéthique*. Brussels: DeBoeck Université, 2001. pp. 665-673.

Sætnan, Ann Rudinow, Heidi Mork Lomell and Carsten Wiecek. 'Controlling CCTV in Public Spaces: Is Privacy the (Only) Issue? Reflections on Norwegian and Danish observations', *Surveillance & Society*, vol. 2, nº 2/3, pp. 396-414.

Scassa, Teresa *et al. An Analysis of Legal and Technological Privacy Implications of Radio Frequency Identification Technologies*, prepared for the Privacy Commissioner of Canada, 28 April 2005.

Smith, Gavin J.D. 'Behind the Screens: Examining Constructions of Deviance and Informal Practices among CCTV Control Room Operators in the UK', *Surveillance & Society*, vol. 2, nº 2/3.

Statistics Canada, *General Social Survey on Victimization, Cycle 18: An Overview of Findings*. Ottawa, Canada, 2004. http://dsp-psd.pwgsc.gc.ca/Collection/Statcan/85-565-X/85-565-XIE.html

Statistics Canada, 'Crime Statistics in Canada, 2005', *Juristat*, 26 nº 4. (July 2006).

Statistics Canada, 'Crime Statistics in Canada, 2006', *Juristat*, 27 nº 5. (July 2007).

Stoddart, Jennifer, 'Surveillance Technologies under Surveillance', Speech, September 2001. http://www.cai.gouv.qc.ca/05_communiques_et_discours/discours_24_09_01-en.html.

Strategic Counsel. *Immigration, Terrorism and National Security*, 7 August 2005.

Strategic Counsel. *Public Perceptions of Immigration and Terrorism*, 9 June 2006.

Surveillance Studies Network. *A Report on the Surveillance Society*. United Kingdom, September 2006. http://www.ico.gov.uk/…/library/data_protection/practical_application/surveillance_society_full_report_2006.pdf.

Thomas, Laurence. 'Autonomie de la personne', *Dictionnaire d'éthique et de philosophie morale*, in Monique Canto-Sperber (dir.). Paris: Presses Universitaires de France, 2001 (1996). pp. 121-124.

U.S. Department of State. 'Department of State Begins Issuing Electronic Passports to the Public', Press release, 14 August 2006.

United Nations Educational, Scientific and Cultural Organisation (UNESCO). *Ethical Implications of Emerging Technologies: A Survey*. Paris: UNESCO, 2007. unesdoc.unesco.org/images/0014/001499/149992E.pdf.

Welsh, Brandon C. and David P. Farrington. *Crime Prevention Effects of Closed Circuit Television: a Systematic Review*, Home Office Research Study 252, August 2002. http://www.homeoffice.gov.uk/rds/pdfs2/hors252.pdf.

Woodward Jr., John D. *et al. Army Biometric Applications: Identifying and Addressing Sociocultural Concerns*. RAND, 2001. http://www.rand.org/publications/MR/MR1237/.

Working Party on the Protection of Individuals with Regard to the Processing of Personal Data of the European Parliament and of the Council of 24 October 1995. 2005. *Working document on data protection issues related to RFID technology*. Brussels: 19 January 2005. http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2005/wp105_en.pdf

Working Party on the Protection of Individuals with Regard to the Processing of Personal Data, *Working Document on Biometrics*. Brussels, Belgium: 1 August 2003.

World Health Organization, *Safety Promotion: Conceptual and Operational Aspects*. September 1998.

Zetter, Kim. 'Hackers Clone E-Passports', *Wired.com*. 3 August 2006. http://www.wired.com/science/discoveries/news/2006/08/71521.

Zureik, Elia, Lynda Harling Stalker and Emily Smith. *Background Paper for the Globalization of Personal Data Project: International Survey on Privacy and Surveillance*. Kingston: Queen's University, 2006.

Appendix 1
Rules for use of surveillance cameras with recording in public places by public bodies

Factors to consider before opting for camera surveillance

1) **Camera surveillance shall be necessary to achieve a specified purpose.**

   It may not be used generally as a public security mechanism. The problem to be solved shall be identified, recurring and circumscribed.

2) **The objective sought by the use of camera surveillance shall be serious and important.**

   The prevention of minor offences or the occurrence of occasional problems cannot justify an invasion of individual privacy. Camera surveillance should not turn out to be an easy solution. In particular, the places targeted must be recognized as a source of criminal activity.

3) **A report shall be produced concerning the concrete risks and real dangers presented by a situation regarding public order and the security of persons, places or property.**

   This report should particularly deal with the following points:

   - the specific, serious and concordant events that have occurred;
   - clear identification of the problem to be solved;
   - the concrete and real public security requirements at stake;
   - the places targeted for camera surveillance and their relation to the grounds invoked;
   - the important, clear and precise objectives that have been identified.

4) **Alternative solutions less prejudicial to privacy should have been considered or tested and have proved difficult to apply or implement or are ineffective.**

   Depending on the problem to be solved and the places concerned, other solutions should have been tested or studied, particularly:

   - the presence of security guards;
   - foot patrols in key locations;
   - the involvement of street workers;
   - accompaniment to the car on request;
   - better lighting of the zone to be protected (streets, parks, corridors, etc.);
   - reinforcement of access doors;
   - installation of protective grilles and alarm systems or marking of objects related to an alarm system;
   - intervention by surveillance personnel;
   - formation of a vigilance committee.

5) **The real impact of camera surveillance shall be measured.**

An analysis of the risks for protection of privacy has been completed;

The advantages and disadvantages of the measure shall be weighed, as well as its potentially perverse or undesirable effects, such as shifting criminal activity to another location. The effectiveness of the measure to correct the situation shall be conclusive.

6) **The public body shall ensure the legitimacy of its objectives so that the purpose of the camera surveillance cannot be diverted or distorted.**

For example, camera surveillance shall not serve:

- to categorize or rank groups of people;
- to establish distinctions based on racial, religious, political or union affiliation or the sexual behaviour of individuals;
- to study human behaviour in order to exercise control over these persons.

7) **The purpose of camera surveillance shall be transparent and explicit.**

The populations concerned shall be consulted and involved before the decision is made. The use of camera surveillance shall have been approved by the accountable authorities of the public body.

8) **Camera surveillance shall be considered in conjunction with at least one of the factors set out in Rule 4 or its equivalent.**

Rules concerning collection of information

9) **The public body shall designate from the outset a person responsible for the collection, retention and communication of data collected by means of camera surveillance.**

At every step, this person shall ensure that these rules are observed.

10) **Camera surveillance shall be adjusted as needed and adapted to the situation. The public body shall set limits for its use.**

The periods of surveillance and eventually of recording, the area covered and the manner in which the operation will be conducted shall be designed to minimize the effects of camera surveillance and preserve the public's privacy as much as possible.

11) **Camera surveillance shall be used only during critical events and for limited periods.**

The use of cameras and recording shall be limited to specific times of day and periods of the year corresponding to the peak periods when crimes usually occur. For example, if it is established that offences are perpetrated on weekends, during the evening or at night, or during public holidays or specific events, camera surveillance shall not extend beyond these periods.

12) **Only the necessary recordings shall be made.**

When a person can permanently view the image captured by a camera, this person shall expect to have reasonable grounds to believe that an offence will be committed to start recording.

If nobody can view the screens continuously, the tape recordings shall be destroyed once they are no longer necessary.

13) The arrangement of the cameras and the type of technology used shall minimize the effects of camera surveillance on people's privacy.

The cameras shall not be directed at private locations, such as a home, building windows, shower rooms, toilet stalls or locker rooms. For this purpose, the new information technology of masking locations shall be adopted to avoid shooting private places or places not concerned by the camera surveillance operation.

The angles of vision, the type of cameras, and the zoom or stop image function shall be evaluated according to the ends sought and the appropriate means of achieving these ends. The same principle applies for use of equipment connected to an alarm or response centre.

14) The persons operating the devices shall be well aware of the rules intended to protect privacy.

The persons shall have received the appropriate training and know the limits imposed by the Act regarding protection of privacy before working as operators. The same principle applies for third parties, i.e. those not directly under the body's authority, in particular those involved by contract in camera surveillance.

15) The public concerned by this surveillance shall be informed by any appropriate notice.

Notices shall announce unequivocally that the place is the object of camera surveillance with recording.

These notices shall:

- be placed in visible locations, at a reasonable distance from the place under surveillance and have the format required by the spatial context;
- mention the object of the camera surveillance and the name of the person responsible.

Rules concerning management of information

16) The equipment used for the recording or recordings shall be protected.

The material recorded shall be the object of precise retention rules to protect the confidentiality of the data.

Security measures shall be implemented to restrict access to the viewing station and the recordings to the persons expressly authorized for this purpose.

A limited number of authorized persons may have access to the premises accommodating the equipment and view the recordings.

17) Use of the recordings shall be limited.

Subject to the exceptions prescribed in the Access Act, the recordings shall not be disclosed to third parties. In this regard, the interconnection of surveillance systems, whether by Internet or otherwise, constitutes disclosure to a third party.

The recordings shall not be the object of associations of images or biometric data, particularly by means of automatic image consultation or facial recognition software.

The recordings shall not be matched, linked or shared with other files, nor serve to constitute data banks.

18) The recording media shall be taken into account in the retention schedule.

The recording media shall be numbered and dated for each site that has been the object of surveillance.

Apart from judicial requirements and police or administrative investigations, the recordings are erased or destroyed as soon as their retention is no longer necessary.

19) A person is entitled to access to the information concerning him.

This person is entitled to access to the recordings made in accordance with the Access Act.

The decision to resort to camera surveillance shall be reviewed periodically

20) The public body shall periodically review (at least on an annual basis) the necessity of its decisions regarding camera surveillance.

The following aspects shall be considered for this purpose:

- the initial grounds still exist;
- the expected results are achieved. Otherwise, the public body must question the actual effects of the process;
- the conditions of use are still adequate and adapted to the situation;
- the appropriateness of the type of cameras used and their number;
- a more appropriate alternative compatible with the right to privacy cannot now be envisioned;
- if applicable, the number of hours of recording per day and the recording periods during the week or the year.

Commission d'accès à l'information du Québec

Appendix 2

OPC Guidelines for the Use of Video Surveillance of Public Places by Police and Law Enforcement Authorities

1) **Video surveillance should only be deployed to address a real, pressing and substantial problem.**

The problem to be addressed by video surveillance must be pressing and substantial, of sufficient importance to warrant overriding the right of innocent individuals to be free from surveillance in a public place. Accordingly, concrete evidence of the problem to be addressed is needed. This should include real evidence of risks, dangers, crime rates, etc. Specific and verifiable reports of incidents of crime, public safety concerns or other compelling circumstances are needed, not just anecdotal evidence or speculation.

2) **Video surveillance should be viewed as an exceptional step, only to be taken in the absence of a less privacy-invasive alternative.**

Less privacy-invasive alternative ways of addressing the identified problem should be chosen unless they are not feasible or significantly less effective.

3) **The impact of the proposed video surveillance on privacy should be assessed before it is undertaken.**

A Privacy Impact Assessment of the proposed video surveillance should be conducted to determine the actual or potential kind and degree of interference with privacy that will result, and the ways in which adverse effects will be mitigated.

4) **Public Consultation should precede any decision to introduce video surveillance.**

Public consultation should be conducted with relevant stakeholders, including representatives of communities that will be affected. "Community" should be understood broadly; it should be recognized that a particular geographic area may have several distinct communities, and one community should not be presumed to speak for the others.

5) **The video surveillance must be consistent with applicable laws.**

Video surveillance must be conducted in accordance with all applicable laws, including overarching laws such as the *Canadian Charter of Rights and Freedoms* and Quebec's *Charter of Human Rights and Freedoms.*

6) **The video surveillance system should be tailored to minimize the impact on privacy.**

The surveillance system should be designed and operated so that the privacy intrusion it creates is no greater than absolutely necessary to achieve the system's goals. For example, limited use of video surveillance (e.g., for limited periods of day, public festivals, peak periods) should be preferred to always-on surveillance if it will achieve substantially the same result.

7) **The public should be advised that they will be under surveillance**

The public should be informed with clearly written signs at the perimeter of surveillance areas, which advise that the area is or may be under surveillance, and indicate who is responsible for the surveillance, including who is responsible for compliance with privacy principles, and who can be contacted to answer questions or provide information about the system.

8) Fair information practices should be respected in collection, use, disclosure, retention and destruction of personal information.

The information collected through video surveillance should be minimal; its use should be restricted, its disclosure controlled, its retention limited, and its destruction assured. If a camera is manned, the recording function should only be turned on in the event of an observed or suspected infraction. If a camera records continuously, the recordings should be conserved for a limited time only, according to a retention schedule, unless they have captured a suspected infraction or are relevant to a criminal act that has been reported to the police. Information collected through video surveillance should not be used for any purpose other than the purpose that the police force or public authority has explicitly stated in the policy referred to in 14 below. Any release or disclosure of recordings should be documented.

9) Excessive or unnecessary intrusions on privacy should be discouraged.

Surveillance cameras should not be aimed at or into areas where people have a heightened expectation of privacy: for example, windows of buildings, showers, washrooms, change rooms, etc. If cameras are adjustable by an operator, reasonable steps should be taken to ensure that they cannot be adjusted or manipulated to capture images in areas that are not intended to be under surveillance.

10) System operators should be privacy-sensitive.

The operators of surveillance systems, including operators hired on contract, should be fully aware of the purposes of the system, and fully trained in rules protecting privacy.

11) Security of the equipment and images should be assured.

Access to the system's controls and reception equipment, and to the images it captures, should be limited to persons authorized in writing under the policy referred to in 14 below. Recordings should be securely held, and access within the organization limited to a need-to-know basis

12) The right of individuals to have access to their personal information should be respected

People whose images are recorded should be able to request access to their recorded personal information. Under many privacy statutes, they have a right of access. Severing the personal information in a recording (including technological blurring or blocking the identities of others) may be necessary to allow individual access. Policies and procedures should be designed to accommodate these requests.

13) The video surveillance system should be subject to independent audit and evaluation.

The system's operations should be subject to frequent audit, and its effectiveness should be evaluated regularly to identify unintended negative effects. Audit and evaluation should be conducted by persons or organizations independent of the management and direction of the video surveillance system. Audits should ensure compliance with the policy governing the system, including ensuring that only pertinent information is collected, that the system is used only for its intended purpose, and that privacy protections in the system are respected. Evaluation should take special note of the reasons for undertaking surveillance in the first place, as determined in the initial statement of the problem and the public consultation, and determine whether video surveillance has in fact addressed the problems identified at those stages. Evaluation may indicate that a video surveillance system should be terminated, either because the problem that justified it in the first place is no longer significant, or because the surveillance has proven ineffective in addressing the problem. Evaluation should take into account the views of different groups in the community (or different communities) affected by the surveillance. Results of audits and evaluations should be made publicly available.

14) The use of video surveillance should be governed by an explicit policy.

A comprehensive written policy governing the use of the surveillance equipment should be developed. The policy should clearly set out:

- the rationale and purpose of the system
- the location and field of vision of equipment
- the rationale and purpose of the specific locations of equipment and fields of vision selected
- which personnel are authorized to operate the system
- the times when surveillance will be in effect
- whether and when recording will take place
- the place where signals from the equipment will be received and monitored, and
- the fair information principles applying to recordings, including
  - security
  - use
  - disclosure
  - retention and destruction
  - rights of individual access to personal information captured, and
  - rights to challenge compliance.

The policy should identify a person accountable for privacy compliance and privacy rights associated with the system. The policy should require officers, employees and contractors to adhere to it, and provide sanctions if they do not. It should provide a process to be followed in the event of inadvertent privacy and security breaches. Finally, it should provide procedures for individuals to challenge compliance with the policy.

15) The public should have a right to know about the video surveillance system that has been adopted.

Police forces and public authorities should recognize that individuals will want information about video surveillance systems. They may seek to know, for example, who has authorized the recording, whether and why their images have been recorded, what the images are used for, who has access to them, and how long they are retained. Police forces and public authorities should be prepared to provide this information.

Office of the Privacy Commissioner of Canada

Commission Consultation and Information Gathering Activities

The *Commission de l'éthique de la science et de la technologie* has heard presentations from the following experts:

Daniel Carpentier, Legal counsel to the *Direction de la recherche et de la planification, Commission des droits de la personne et des droits de la jeunesse (CDPDJQ)*

Sylvie Laflamme, Administrative Manager of the Québec Chapter, Canadian Security Association (CANASA)

Sylvain Lemay, Inspector, *Division de la qualité des services, Service de police de la Ville de Montréal (SPVM*)

Bruno Leclerc, Professor, *Département des sciences humaines, programmes d'études supérieures en éthique, Université du Québec à Rimouski (UQAR);* Director of Ethos Research Group

André Beauchamp, Environmental consultant

Julie-Anne Boudreau, Professor-researcher, *INRS – Urbanisation, Culture et Société*; Chairholder, Canada Research Chair in the City and Issues of Insecurity

In December 2007, the following experts accepted to conduct a critical reading of the working committee's preliminary report.

Jean-Philippe Racicot, Analyst, Privacy Council Office

Sami Aoun, Tenured Professor, *École de politique appliquée, Faculté des lettres et sciences humaines, Université de Sherbrooke*

Daniel Carpentier, Legal counsel to the *Direction de la recherche et de la planification, Commission des droits de la personne et des droits de la jeunesse du Québec (CDPDJQ)*

Clément Robitaille, *Ministère de la Sécurité publique (MSP)*

Hervé Fischer, Associate Professor, *Université du Québec à Montréal (UQAM);* Founder and Director, International Digital Observatory

Patrice St-Gelais, Information technology advisor, *Commission d'accès à l'information (CAI)*

The Commission wishes to thank everyone for their valuable contribution to the development and content of this Position statement.

Events

- *Terra Incognita, Privacy Horizons*, 29th Conference of Data Protection and Privacy Commissioners, Montréal, September 25th to 28th, 2007.

Commission Members[238]

President

Édith Deleury
Professor – Faculté de droit
Université Laval

Members

Frédéric Abraham
Doctoral Candidate
Université du Québec à Trois-Rivières

Patrick Beaudin
Director General
Société pour la promotion de la science
et de la technologie

Dr Pierre Deshaies
Community Health Specialist
Chef du Département clinique de santé publique
Hôtel-Dieu de Lévis

Hubert Doucet
Programmes de bioéthique
Université de Montréal

Benoît Gagnon
Researcher
Centre international de criminologie comparée (CICC)
Université de Montréal

Jacques T. Godbout
Sociologist
Institut national de la recherche scientifique –
Urbanisation, Culture et Société

Patrice K. Lacasse
Coordinator of the Bureau de développement social
des Premières Nations du Québec
Commission de la santé et des services sociaux
des Premières Nations du Québec et du Labrador

François Pothier
Professor
Faculté des sciences de l'agriculture et de l'alimentation
Université Laval

Dany Rondeau
Professor
Département des sciences humaines
Université du Québec à Rimouski

Andy Sheldon
President and Chief Executive Officer
Medicago inc.

Eliana Sotomayor
École de service social
Université de Montréal

Guest Member

Danielle Parent
Directrice des affaires juridiques
Commissaire au lobbyisme du Québec

Coordinator

Nicole Beaudry, notary

238. As of the adoption of this Position statement.

Mass surveillance can be considered a fact of modern society. Its significance is reflected in the variety of methods used to collect information. Among these methods, New Surveillance and Monitoring Technologies (NSMT), and particularly the way in which they are used, raise a number of ethical issues. In addition, the Commission de l'éthique de la science et de la technologie (CEST) has taken on the mandate of formulating an opinion on technology which could be used in mass surveillance for purposes of security : Biometric Systems, Video Surveillance and Radio-Frequency Identification (RFID).

In Search of Balance : An Ethical Look at New Surveillance and Monitoring Technologies for Security Purposes is the Commission's fifth Position statement. A look at the notions of security, sense of insecurity, risk, and surveillance is followed by a technical and ethical overview of each NSMT under consideration. Fundamental democratic values are at the heart of the ethical issues involved : Assessment of the effectiveness and reliability of NSMT, proportionality of response to insecurity, social acceptability, consent, respect for end purpose, and protection of personal information.

This Position statement is available at : www.ethique.gouv.qc.ca

The CEST's mission firstly consists in informing, sensitizing, gathering opinion fostering reflection, and organizing debates on the ethical issues raised by developments in science and technology and, secondly, proposing orientations to guide stakeholders in their decision-making.

Commission
de l'éthique
de la science
et de la technologie
Québec