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

SUMMARY AND RECOMMENDATIONS

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

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.**

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.