29E CONFÉRENCE INTERNATIONALE DES COMMISSAIRES
À LA PROTECTION DES DONNÉES ET DE LA VIE PRIVÉE

LES HORIZONS DE LA PROTECTION DE LA VIE PRIVÉE

TERRA INCOGNITA

PRIVACY HORIZONS

29TH INTERNATIONAL CONFERENCE OF
DATA PROTECTION AND PRIVACY COMMISSIONERS

Atelier
Dragon : *Quand la loi rencontre la technologie*
Les normes

Workshop
"Law Meets Technology" Dragon
Standards

26 septembre/Septembre 26

Série Terra Incognita, cahier de travail # 5/Terra Incognita, workbook series # 5

Office of the Privacy Commissioner of Canada
Commissariat à la protection de la vie privée du Canada

Table des matières / Table of contents

Biographies

Président : M. John Borking

Ancien commissaire à la protection de la vie privée des Pays-Bas (1994-2006), John Borking est directeur de Borking Consultancy, bureau d'experts-conseils dont il est le seul employé. Il se spécialise dans la protection des renseignements personnels et les modes alternatifs de règlement des conflits, à l'aide de moyens électroniques. M. Borking participe à divers projets de recherche liés à la protection des renseignements personnels, dont PRIME (Gestion de l'identité et des renseignements personnels pour l'Europe), EUROPRISE (sceaux de protection), celui du groupe de recherche hollandais PAW (protection des renseignements personnels dans un monde ambiant) et celui du groupe de recherche norvégien PETWEB (les technologies d'amélioration de la confidentialité pour application Web). Ces initiatives portent sur des sujets aussi diversifiés que l'identification par radiofréquence, les agents informatiques et les essais pour créer un environnement de cyberimmunité autour d'une personne en vue de protéger la vie privée et d'améliorer la sécurité dans un monde ambiant. Il est secrétaire général de la Wroclaw Foundation qui s'occupe de normalisation de la protection de la vie privée et des technologies d'amélioration de la confidentialité (TAC). Il a publié et il continue d'écrire de nombreux livres et articles sur la protection de la vie privée et les technologies d'amélioration de celle-ci, la protection de logiciels, le droit de l'informatique, les jeux électroniques, les modes alternatifs de règlement des conflits et la cybermédiation.

Conférenciers

M. Colin Bennett, Ph. D.

Colin Bennett a fait son baccalauréat et sa maîtrise à l'Université de Wales et son doctorat à l'Université de l'Illinois à Urbana-Champaign. Depuis 1986, il enseigne au Département de science politique de l'Université de Victoria, où il est aujourd'hui professeur. De 1999 à 2000, il a été boursier de la Harvard's Kennedy School of Government. En 2007, il a obtenu une bourse de recherche scientifique au Center for the Study of Law and Society à l'Université de Californie, à Berkeley. Ses recherches ont porté sur l'analyse

Biographies

Chair : Mr. John Borking

A former Privacy Commissioner for the Netherlands (1994 – 2006), John Borking is Director of Borking Consultancy, a one man consultancy firm on privacy protection and e-ADR (alternative dispute resolution). Mr. Borking currently participates in a number of privacy-related research initiatives including PRIME (Privacy and Identity management for Europe), EUROPRISE (privacy seals), the Dutch research group PAW (Privacy in an Ambient World) and the Norwegian research group PETWEB (PET for web applications). These initiatives cover topics as diverse as RFIDs, software agents, and trying to create an e-immunity environment around a person for protecting privacy and enhance security in the ambient world. He is general secretary of The Wroclaw Foundation dealing with standardization of privacy and PET technologies. He is and has been (co-) author of many books and articles about privacy and privacy enhancing technologies, software protection, computer law, e-gaming, alternative dispute resolution and e-mediation.

Speakers

Dr. Colin Bennett

Colin Bennett received his Bachelor's and Master's degrees from the University of Wales, and his Ph.D from the University of Illinois at Urbana-Champaign. Since 1986 he has taught in the Department of Political Science at the University of Victoria, where he is now Professor. From 1999-2000, he was a fellow at Harvard's Kennedy School of Government. In 2007 he was a Visiting Fellow at the Center for the Study of Law and Society at University of California, Berkeley. His research has focused on the

comparative des technologies de surveillance et des politiques sur la protection de la vie privée à l'échelle nationale et internationale. En plus d'avoir publié de nombreux articles dans des revues scientifiques et des journaux, il a écrit trois livres : *Regulating Privacy: Data Protection and Public Policy in Europe and the United States* (Cornell University Press, 1992); *Visions of Privacy: Policy Choices for the Digital Age* (University of Toronto Press, 1999, avec Rebecca Grant); *The Governance of Privacy: Policy Instruments in the Digital Age* (Ashgate Press, 2003; MIT Press, 2006 avec Charles Raab).

M. John P. Hopkinson

John P. Hopkinson est stratège en sécurité, EWA Information et Infrastructure Technologies Inc. et président de l'ISSEA (International Systems Security Engineering Association).
Il s'est joint à l'IIT en mai 2001. Il est responsable des normes de même que des liens et des activités avec le consortium. Il élabore des stratégies et les plans d'action pour les mettre en œuvre. Fort de plus de 35 années d'expérience dans le domaine de la sécurité, tant dans le secteur militaire que commercial, il a poursuivi des recherches sur divers aspects de la sécurité et de la technologie de l'information. Il a été l'un des principaux collaborateurs lors de l'élaboration du SSE-CMM, et de l'ISO/IEC 21827. Il est président du Comité technique des technologies de l'information, chef de la délégation canadienne auprès du Comité technique de l'Organisation internationale de normalisation (ISO/IEC JTC 1), membre du Conseil des gouverneurs universitaires du Système international de certification des professionnels des systèmes de sécurité, membre de ISO/IEC JTC 1/SC 27 et membre du Comité canadien sur les normes ISO. L'Association canadienne de normalisation lui a décerné le Prix du mérite, et le prix du leadership lui a été remis par le Conseil canadien des normes.

M. John Sabo

John Sabo, CISSP, est directeur des relations avec le gouvernement (Global Government Relations) pour CA Inc., où il apporte son expertise en ce qui concerne l'utilisation de technologies de l'entreprise CA dans diverses infrastructures dignes de confiance, et dirige des

comparative analysis of surveillance technologies and privacy protection policies at the domestic and international levels. In addition to numerous scholarly and newspaper articles, he has published three books: *Regulating Privacy: Data Protection and Public Policy in Europe and the United States* (Cornell University Press, 1992); *Visions of Privacy: Policy Choices for the Digital Age* (University of Toronto Press, 1999, with Rebecca Grant); *The Governance of Privacy: Policy Instruments in the Digital Age* (Ashgate Press, 2003; MIT Press, 2006 with Charles Raab).

Mr. John P. Hopkinson

John P. Hopkinson is Security Strategist, EWA Information & Infrastructure Technologies Inc., an EWA Company and President, ISSEA (International Systems Security Engineering Association). Mr. Hopkinson joined /IIT in May 2001 and is responsible for Standards and Consortia activities and liaison. He develops strategies and action plans to fulfill those strategies. John Hopkinson has over 35 years of experience in the security field in the military and commercial sectors. He has conduced research in many areas related to information technology security. Mr. Hopkinson was a key contributor to the development of the SSE-CMM, ISO/IEC 21827. He is the Chairman of the Technical Committee on Information Technology, Head of the Canadian Delegation for ISO/IEC JTC 1, he is a Member of the Academic Board of the International Systems Security Professional Certification Scheme, Member of ISO/IEC JTC 1/ SC 27 and a Member of the Canadian National Committee on ISO. He has received the Award of Merit from the Canadian Standards Association and the Leadership Award form the Standards Council of Canada.

Mr. John Sabo

John Sabo, CISSP, is Director, Global Government Relations for CA, Inc., providing expertise in the use of CA technologies in trusted infrastructures and leading internal and external security and privacy initiatives. Mr. Sabo is a member of the Department of Homeland

initiatives internes et externes en matière de sécurité et de protection des renseignements personnels. M. Sabo est membre du Data Privacy and Integrity Advisory Committee du département de la Sécurité intérieure des États-Unis et occupe un grand nombre de postes de direction dans l'industrie : président de l'International Security, Trust, and Privacy Alliance (ISTPA), président de l'Information Technology-Information Sharing and Analysis Center (IT-ISAC), président de l'ISAC Council, membre de l'IT Sector Coordinating Council et membre de l'OASIS IDtrust Member Section Steering Committee. Avant de travailler dans le secteur privé, M. Sabo était directeur du personnel des services électroniques de la Social Security Administration des États‑Unis, où il était chargé de la politique de sécurité et de confidentialité en ligne et de questions d'ordre opérationnel. M. Sabo est diplômé de King's College (Pennsylvanie) et de la University of Notre Dame. Il est également reconnu comme Certified Information Systems Security Professional (CISSP).

Security's Data Privacy and Integrity Advisory Committee and serves in a number industry leadership positions: President, International Security, Trust, and Privacy Alliance (ISTPA); President, Information Technology-Information Sharing and Analysis Center (IT-ISAC); Chair, ISAC Council; member, IT Sector Coordinating Council; and member, OASIS IDtrust Member Section Steering Committee. Prior to his work in the private sector, Mr. Sabo was Director of the Social Security Administration's Electronic Services Staff, where he addressed online security and privacy policy and operational issues. Mr. Sabo holds degrees from King's College (Pennsylvania) and the University of Notre Dame, and is a Certified Information Systems Security Professional (CISSP).

29E CONFÉRENCE INTERNATIONALE DES COMMISSAIRES
À LA PROTECTION DES DONNÉES ET DE LA VIE PRIVÉE

LES HORIZONS DE LA PROTECTION DE LA VIE PRIVÉE

TERRA INCOGNITA

PRIVACY HORIZONS

29TH INTERNATIONAL CONFERENCE OF
DATA PROTECTION AND PRIVACY COMMISSIONERS

« Dire ce que l'on fait et faire ce que l'on dit » : Arguments et observations en faveur d'une norme internationale de protection des renseignements personnels

"Saying what you do and Doing what you say": Arguments and Prospects for an International Privacy Standard

Par/by:

Colin J. Bennett et/and Robin Bayley

Juillet 2007/July 2007

Office of the Privacy Commissioner of Canada

Commissariat à la protection de la vie privée du Canada

I. Introduction

Un réseau et un discours se sont forgés au fil des trente dernières années autour des concepts de la vie privée et de la protection des données. Les préoccupations profondes et grandissantes ont motivé la mise en place de politiques en raison de l'« érosion » des droits fondamentaux de la personne devant la puissance de la bureaucratie et de la technologie. En même temps avait lieu l'expansion du réseau de professionnels et un discours de plus en plus prégnant chez les personnes œuvrant dans le milieu de la normalisation en ce qui concerne la notion de l'« assurance qualité ». En règle générale, ces deux mondes se sont rarement entrecroisés. Chacun d'eux témoigne de ses prévisions, de ses institutions, de ses pratiques et d'un langage qui lui est propre. L'objectif de ce document est de retracer l'historique des tentatives de réunification de ces deux univers, et de proposer des moyens par lesquels les institutions et les personnes œuvrant dans le milieu de la normalisation pourraient contribuer à la mise en œuvre des droits et responsabilités relativement à la protection de la vie privée, au sein d'organisations complexes relevant des secteurs public ou privé.

Dans les années 1970 et 1980, dans plusieurs pays du monde, on présumait généralement qu'une loi pour la protection des renseignements personnels (protection des données) était le seul instrument requis pour garantir la protection de tels renseignements dont l'application était assurée par une autorité indépendante de protection des données[1]. Dans les années 1990, cette opinion s'est modifiée. La législation était toujours considérée comme étant un élément nécessaire, mais elle n'était plus suffisante pour résoudre la multitude de problèmes liés aux renseignements personnels, problèmes éprouvés dans un monde de plus en plus branché et dans un environnement en ligne. Les solutions proposées ont alors fait appel à d'autres instruments d'autorégulation et relevant de la technologie : les codes de pratique, les programmes concernant les sceaux de confidentialité, les technologies destinées à protéger la vie privée et l'évaluation des facteurs relatifs à la vie privée. C'est dans ce contexte qu'a germé l'idée d'une norme de gestion en matière de protection des renseignements personnels[2].

Dans cet article, nous exposerons les raisons qui justifient l'établissement de normes générales de

I. Introduction

A network and a discourse have grown up over the last 30 years surrounding the concepts of privacy and data protection. Policies have generally emerged out of a profound and widespread concern about the erosion of a fundamental human right in the face of some powerful bureaucratic and technological forces. At the same time, there has been a similarly expanded network and growing discourse in the standards community surrounding the notion of "quality assurance." For the most part, these worlds have not intersected. Each has its own assumptions, institutions, practices and language. The purpose of this paper is to trace the history of the attempts to bring these worlds together, and to suggest ways in which the institutions and skills of the standards community might contribute to the implementation of privacy rights and responsibilities in complex public and private organizations.

In the 1970s and 1980s, it was commonly presumed in many areas of the world, that the only instrument necessary for the protection of personal information was an information privacy (data protection) law, overseen by an independent data protection authority.[1] In the 1990s, those assumptions changed. Legislation was then seen as a necessary but not sufficient condition for resolving the myriad personal information problems encountered in a globally connected and networked environment. Other self-regulatory and technological instruments also had to be part of the solution: codes of practice, privacy seal programs, privacy-enhancing technologies and privacy impact assessments. This is the context in which the idea of a management standard devoted to the protection of personal information arose.[2]

This paper first outlines the rationale for general management standards and how they intersect with the requirements for responsible privacy and data protection. It then outlines the rationale for a separate management standard devoted solely to protecting privacy, and traces the various attempts to develop such a privacy standard through the Canadian Standards Association (CSA) and subsequently through the International Organization for Standardization (ISO), the European Committee for Standardization/Information Society Standardization System (CEN/ISSS) and the International Security, Trust, and Privacy Alliance (ISTPA). The paper concludes that the rationale for an international privacy management standard

gestion et la façon dont ces normes s'entrecroisent avec les exigences relatives à la protection adéquate de la vie privée et la protection des données. Nous présenterons ensuite les motifs justifiant une norme de gestion distincte qui s'appliquerait uniquement à la protection de la vie privée et nous décrirons les différentes tentatives d'élaboration d'une telle norme sur la vie privée, par l'entremise de l'Association canadienne de normalisation (CSA), l'Organisation internationale de normalisation (ISO), le Système de normalisation de la société de l'information du Comité européen de normalisation (CEN-ISSS) et le International Security, Trust, and Privacy Alliance (ISTPA). Ce document conclut que les motifs en faveur d'une norme de gestion internationale de la protection de la vie privée sont solides mais que les nombreux projets entrepris ne se sont traduits que par peu de réalisations concrètes. Nous en indiquons les raisons et proposons quelques pistes pour l'ensemble des autorités de protection des données.

II. Les normes de gestion : peuvent-elles favoriser la protection des données?

Les réponses apportées à deux groupes de questions préliminaires ont servi à déterminer si les normes de gestion pouvaient assurer la protection des données. Premièrement, jusqu'à quel point les systèmes actuels d'assurance qualité[3] permettent-ils de promouvoir les principes de la protection des données tout en facilitant le travail de vérification de la conformité des autorités de protection des données? Deuxièmement, existe-t-il un exemple distinct pour une norme de gestion indépendante qui pourrait, pour certaines organisations, « faire le pont »[4] avec les critères d'enregistrement d'une norme actuelle d'assurance qualité comme, par exemple, ISO 9001?

Pendant plusieurs années, les personnes œuvrant dans le domaine de la protection de la vie privée et des données – les autorités de réglementation, les universitaires, les consultants et les avocats – ont souligné l'importance de l'instauration d'une « culture de la vie privée » au sein des organisations[5], ce qui signifie habituellement que les principes de protection des données et de la vie privée ne peuvent être imposés par une personne ou un organisme externe; ces principes doivent être considérés à l'interne comme étant

is powerful but that much activity has yielded few real achievements. It suggests the reasons and provides some ways forward for the community of data protection authorities.

II. What can management standards contribute to data protection?

Two sets of preliminary questions have to be answered in order to address the contribution of management standards to data protection. Firstly, to what extent can existing quality assurance systems[3] promote the principles of data protection and thereby assist the compliance work of data protection authorities? Secondly, is there a separate case for a stand-alone management standard which could, for some organizations, be "bridged"[4] to the registration of an existing quality assurance standard, like ISO 9001?

For many years the privacy and data protection community–regulators, academics, consultants and advocates–have insisted on the importance of building a "culture of privacy" within organizations.[5] This normally means that privacy and data protection principles cannot be imposed from without; they have to be seen internally as the 'right thing to do'. There must be a public commitment to the information privacy principles, as well as to the organization's processes and values to ensure that they are carried out.

In the words of standards bodies, organizations should "say what they do and do what they say". The ISO 9000 family of quality assurance standards essentially embodies a series of documents that require organizations to:

- Document what they do
- Perform to that documentation
- Ensure the process is effective
- Record the results of the work [6]

The ISO 9000 series was first produced in 1987, updated in 1994 and further revised in 2000, when the generic standard (ISO 9001) consolidated the requirements of a number of older standards in the series. The 2000 version placed a stronger emphasis on 'process management' and monitoring of internal tasks and activities, rather than just inspecting the final product. "Generic" means that the same standards can be applied to any organization, regardless of size, activity or product. These standards apply to the entire management

les « bonnes actions à poser ». Cela suppose un engagement public en vue de respecter les principes liés aux renseignements personnels, ainsi que les valeurs et les processus de l'organisation, afin de s'assurer qu'ils soient mis en application.

Pour reprendre les termes utilisés par les organismes rédacteurs de normes, les organisations doivent « dire ce qu'elles font et faire ce qu'elles disent ». L'ensemble des normes d'assurance qualité de type ISO 9000 englobe essentiellement une série de procédures qui font en sorte que les organisations sont dans l'obligation de :

- documenter ce qu'elles font;
- produire cette documentation;
- s'assurer que le processus est efficace;
- consigner les résultats des travaux[6].

La série de normes ISO 9000 a été élaborée en 1987; ces normes ont fait l'objet d'une mise à jour en 1994 et d'une révision en profondeur en 2000, alors que la norme générique (ISO 9001) regroupait des exigences pour un certain nombre d'anciennes normes de cette série. La version de l'année 2000 met davantage l'accent sur la « gestion des processus » et sur le contrôle des tâches et des activités réalisées à l'interne, plutôt que sur la simple inspection du produit final. Le terme « générique » signifie que les mêmes normes peuvent être appliquées dans n'importe quelle organisation, peu importe la taille, les activités ou le produit qu'elle fabrique. Ces normes s'appliquent à la totalité du système de gestion et soutiennent un certain nombre de caractéristiques essentielles que toute organisation doit mettre en œuvre, aux fins d'enregistrement de cette dernière en vue d'obtenir le sceau de « gestion de la qualité totale ». Les mêmes principes s'appliquent au système équivalent des normes en matière de processus environnemental, dans le cadre de la série de normes ISO 14000.

De plus en plus d'organisations, tant dans le secteur public que le secteur privé, reconnaissent les bienfaits de l'enregistrement relativement à la gestion de la qualité[7]. Un sondage réalisé en 2004 a dévoilé qu'à la fin de cette année-là, le nombre total de certifications ISO 9000 émises à l'échelle mondiale s'élevait à 670 399, une augmentation de 172 480 par rapport à l'année précédente. Le nombre de pays dans lesquels des certifications

system and bear a number of essential features which any organization has to implement if it wants the registration and the cachet of "total quality management". The same principles apply to the equivalent system of environmental process standards within the ISO 14000 series.

More and more organizations, in both public and private sectors, are recognizing the benefits of quality management registration.[7] A survey in 2004 demonstrated that by the end of that year, the worldwide total of ISO 9000 certificates was at 670,399, an increase of 172,480 over the previous year. The number of countries in which ISO 9000 certificates have been issued is now 154.[8] It is also commonly assumed that quality assurance systems apply solely to the private sector. But an increasing number of public sector agencies are also seeing the benefits of ISO 9001 registration– for instance, many organizations in the health care sector. Independent studies have demonstrated an improvement of patient care without leading to excessive bureaucracy.[9] Universities, schools and local governments have also seen the benefits.

Quality assurance methods are, therefore, global in character, applicable in all sectors and seemingly on the increase.

The following is a brief explanation of the ISO quality assurance process. According to one report, ISO 9000 quality assurance:

- Provides the means for staff to perform their tasks at the right time;
- Provides the means for identifying the right tasks and specifying them in a way that will yield the right results;
- Provides the means for documenting the company's experience in a structured manner and thus establishing a basis for educating and training staff and the systematic improvement of performance;
- Provides objective evidence that can be used to demonstrate the quality of the company's products and services, and that its operations are under control to assessors, customers' representatives, etc.;
- Reduces "fire fighting" and thus frees managers from having to intervene constantly in business operations;
- Helps maintain consistency in the quality of products or services;
- Brings clarity and transparency to duties and responsibilities;

ISO 9000 ont été émises est maintenant de 154[8]. Il est généralement admis que les systèmes d'assurance qualité s'appliquent uniquement au secteur privé. Cependant, un nombre croissant d'agences du secteur public constatent également les avantages de s'enregistrer à la norme ISO 9001 (c'est le cas, par exemple, de plusieurs organisations relevant du secteur des soins de santé). Des études indépendantes ont démontré qu'il y avait eu une amélioration des soins aux patients, sans un alourdissement de la bureaucratie[9]. Les universités, les maisons d'enseignement et les administrations municipales ont aussi pu en constater les avantages.

Les méthodes relatives à l'assurance qualité peuvent, par conséquent, être mises en application à l'échelle mondiale, dans tous les secteurs, et semblent être adoptées de plus en plus.

Voici une brève description du processus d'assurance qualité ISO. Selon un rapport, l'assurance qualité ISO 9000 :

- fournit aux membres du personnel des moyens d'accomplir leurs tâches, en temps opportun;
- fournit des moyens pour déterminer quelles sont les tâches adéquates et décrit celles-ci de façon à atteindre les bons résultats;
- fournit des moyens pour documenter l'expérience de l'entreprise, de façon structurée et ainsi établir les bases pour la sensibilisation et la formation du personnel de même que pour l'amélioration systématique du rendement;
- fournit des preuves tangibles qui peuvent être utilisées pour confirmer la qualité des produits et services de l'entreprise et pour démontrer aux évaluateurs, aux représentants des consommateurs, etc., que les opérations sont sous contrôle;
- permet de diminuer le nombre de problèmes urgents à résoudre, ce qui libère les gestionnaires qui n'ont plus à intervenir constamment relativement au fonctionnement de l'entreprise;
- favorise le maintien de l'uniformité en matière de qualité des produits ou des services;
- permet plus de clarté dans la description des tâches et plus de transparence quant aux responsabilités;
- améliore la traçabilité (permet de suivre un produit aux différentes étapes de sa

- Improves traceability (material can be traced at any stage from procurement to every stage of processing and final delivery to customer).[10]

Of course, no one quality assurance system is like another; the organization is obliged to tailor the standard to its own processes and functions. The general requirements set out in ISO 9001 (a relatively brief 12 pages), need to be interpreted and set out in a quality manual for each organization. Each organization indicates how it will implement the requirements and outlines this in a manual which guides the development of a set of prescriptive procedures for each unit of the organization. It is this documentation which forms the basis of quality planning and review, and internal audit. Organizations are then generally registered by a professionally accredited third party (a registrar)[11] whose auditors determine whether the quality system criteria have been successfully met. Registrars can be special units in large accounting/ consultancy firms, stand-alone specialized firms, or a body within a national standards organization, such as the Quality Management Institute in Canada.

Once registered, each organization (or system within an organization) is subject to periodic audits of sections of its operation, and usually a full-scale re-audit every three years, or a rolling audit of a third of its operations every year. Thus the quality assurance process is dynamic and organizations are expected to review their systems continually and make appropriate adjustments to the registration if there is a dramatic change in operations.[12]

Therefore, it is plausible to contend that those organizations that have gone through ISO 9001 quality assurance are less likely to experience breaches of personal data and other privacy scandals, for a number of reasons, including:

- The organization will have undergone thorough internal and external audits and should therefore be aware of its various operating systems and what personal data they hold.
- The organization is less likely to suffer from the "left hand not knowing what the right hand is doing" problem, so often encountered when organizations are exposed for flouting privacy standards. Total quality management should at least give top management a comprehensive overview of operations and a regular process for fixing problems.
- Staff will have undergone training.

production, de sa transformation et de sa commercialisation)[10].

Bien entendu, aucun système d'assurance qualité ne ressemble à un autre; l'organisation se voit donc dans l'obligation d'adapter la norme en fonction de ses propres processus et de ses propres activités. Les exigences d'ordre général définies dans la norme ISO 9001 (une norme relativement courte de 12 pages), doivent être interprétées et établies dans un manuel qualité et ce, pour chaque organisation. Chacune d'elle précise comment elle entend mettre en œuvre les exigences décrites dans un manuel qui donne des points de repère pour l'élaboration d'un ensemble de procédures normatives pour chacune des unités de l'organisation. Ces documents sont à la base de la planification et de la révision de la qualité, ainsi que de l'audit interne. Les organisations sont ensuite généralement enregistrées par une tierce partie professionnelle accréditée (un registraire)[11] dont les vérificateurs déterminent si les critères du système de qualité ont été respectés. Les registraires peuvent être des unités spéciales d'importants cabinets comptables ou de firmes de consultants, de firmes spécialisées indépendantes ou encore une instance au sein d'une organisation nationale d'établissement de normes, telle que le Quality Management Institute au Canada.

Lorsqu'elle est enregistrée, chaque organisation (ou chaque système d'une organisation) fait l'objet de vérifications périodiques de segments de ses opérations, et fait habituellement l'objet d'une vérification exhaustive à tous les trois ans ou d'une vérification du tiers de ses opérations annuellement. Ainsi, le processus d'assurance qualité est dynamique et l'on s'attend à ce que les organisations revoient régulièrement leurs systèmes et effectuent les ajustements appropriés à l'enregistrement si les opérations subissent des changements considérables[12].

Par conséquent, nous pouvons dire que ces organisations, qui se sont enregistrées à l'assurance qualité de la norme ISO 9001, sont moins susceptibles d'être aux prises avec des problèmes liés à une brèche dans la protection des renseignements personnels ou liés à tout autre scandale provoqué par une brèche dans la protection de la vie privée, pour un certain nombre de raisons, dont le fait que :

- l'organisation a réalisé des vérifications

- While documenting their processes for registration, organizations are required to examine and address any regulatory requirements.
- Outside expertise is brought in during auditing to obtain registration, and auditors have the opportunity to alert the organization to areas where there is room to improve their practices.

There are indeed more explicit parallels between the existing ISO 9001 framework and privacy and data protection principles, especially for those personal data intensive organizations whose purpose is the delivery to clients of accurate personal data. For companies in the data brokerage, credit-reporting, and direct-marketing industries, their "product" is personal data. Total quality management can assure suppliers and clients that these data are accurate, up-to-date and complete; that appropriate security safeguards are in place; and that there are appropriate retention schedules, among others. In short, quality assurance can help establish that the organization is accountable and responsible for the personal data in its custody–the principal assumption behind most data protection regimes.

Contemporary privacy auditors and consultants essentially think in very similar and holistic "quality assurance" terms, even if they are not explicit, or even cognizant of this approach. The Ponemon Institute in the United States, for instance, extols "Responsible Information Management" – "a process for ensuring trust and confidence in how a company's leaders conduct business. Specifically, it has to do with the alignment of the privacy preferences of key stakeholders–such as consumers, employees and the general public–with business, data and technology."[13]

Quality assurance can test whether procedures are in place for interacting with consumers, as well as business clients. For example, the receipt, processing and response to customer complaints are central components of a quality assurance system for many companies. There are "quality" ways to set up a complaints resolution process, and there are "less quality" ways. There are established quality procedures for linkage between a system of individual complaint resolution and the analysis of larger systemic problems. There is nothing inherently different between effective complaints resolution for faulty widgets, and complaints resolution concerning the mistreatment of personal information.

internes et externes approfondies et devrait par conséquent connaître ses différents systèmes d'exploitation et les renseignements personnels qui y sont conservés;
- l'organisation risque moins de connaître des problèmes découlant du fait que « la main gauche ignore ce que fait la main droite », problèmes qui se manifestent très souvent quand les organisations sont susceptibles de faire fi des normes de protection de la vie privée. La gestion de la qualité totale devrait au moins procurer à la haute direction un bon aperçu des opérations et un processus régulier pour résoudre les problèmes;
- le personnel a suivi une formation;
- en documentant leurs processus aux fins d'enregistrement en vue de se conformer à une norme, les organisations doivent examiner et tenir compte de toutes les exigences réglementaires;
- on a recours à l'expertise d'un tiers au cours de la vérification aux fins d'enregistrement et les évaluateurs ont l'occasion d'aviser l'organisation concernant les secteurs qui pourraient améliorer leurs pratiques.

À vrai dire, il existe de nombreux parallèles explicites entre le cadre existant pour la norme ISO 9001 et les principes de protection des données et de la vie privée, plus particulièrement ceux des organisations qui détiennent davantage de renseignements personnels et qui transmettent à leurs clients des renseignements personnels précis. Quant aux entreprises œuvrant dans le courtage de données, aux agences d'évaluation du crédit, ainsi qu'aux industries de marketing direct, leurs « produits » sont constitués de renseignements personnels. La gestion de la qualité totale permet entre autres de garantir aux fournisseurs et aux clients que ces données sont exactes, à jour et complètes; les mesures de sécurité adéquates sont en place; les périodes de conservation des données sont appropriées. Bref, l'assurance qualité aide à déterminer si l'organisation est responsable des renseignements personnels qu'elle détient et qu'elle conserve, ce qui correspond précisément à l'hypothèse formulée concernant la plupart des mécanismes de protection des données.

De nos jours, les vérificateurs et les consultants œuvrant dans le domaine de la protection de la vie privée raisonnent principalement en termes holistiques et similaires d'« assurance qualité » même s'ils ne sont pas explicites ou même s'ils ne

Of course, quality assurance standards cannot serve as a substitute for law which is crucial in establishing the general lines which organizations cannot cross. However, once legal rules for privacy protection are established, (as indeed they are in the vast majority of advanced industrial states), then the critical task is to ensure that declared data protection or privacy policies are implemented throughout an organization. A standards registration process whereby organizations say what they do, and have their practices verified to determine if they do what they say, could potentially become one of the various "policy instruments" within the toolbox of data protection officials.

III. The Rationale for a Privacy Management Standard

Much of contemporary data protection implementation is about transparency – internally to management and staff, and externally to data subjects and regulators. In the 1990s, a number of privacy and data protection experts began to realize that using an international quality assurance standard could contribute to resolving the perennial problem of trying to determine what actually happens to personal data within complex organizations. The experts also recognized that although privacy is a fundamental human right, it is also one that entails implementation in complex organizations.

Thus in the terms of fair information principles[14], management standards can:

- Promote transparency of organizational policy and purposes
- Improve and verify the procedures for interacting with data subjects (complaint resolution, access requests, and consent provisions)
- Improve and verify internal procedures for personal data management (data security, data quality, and data retention)

Several factors motivated this community to begin thinking about the possibility of using standards as one of the instruments in the privacy toolkit.

First, there was a broad recognition that consumer concerns about privacy and security had to be properly satisfied during the development and integration of global electronic commerce in the mid-to late 1990s. This recognition raised the problem of determining the comparability of pri-

connaissent pas cette approche. Par exemple, le Ponemon Institute, sis aux États-Unis, vante la « gestion responsable de l'information » – « un processus visant à assurer la confiance et la confidentialité quant à la façon dont les dirigeants d'une entreprise assurent la réalisation des opérations. Il s'agit plus particulièrement d'harmoniser les préférences des principaux intervenants en protection de la vie privée – tels que les consommateurs, les employés et le grand public – relativement aux affaires, aux données et à la technologie »[13] [traduction].

L'assurance qualité permet de vérifier si les procédures sont en place pour les communications avec les consommateurs, ainsi qu'avec les clients. Par exemple, la réception, le traitement et le règlement des plaintes des consommateurs sont des éléments centraux du système d'assurance qualité de plusieurs entreprises. Il existe des mécanismes « de qualité » pour mettre en œuvre un processus de règlement des plaintes et il existe des mécanismes de « moindre qualité ». Des procédures ont été mises en œuvre en matière de qualité de sorte qu'il soit possible d'établir des liens entre un système de règlement des plaintes et l'analyse de problèmes plus importants touchant un système. Il n'y a fondamentalement aucune différence entre le règlement efficace des plaintes concernant un bien défectueux et le règlement des plaintes relativement au traitement négligent de renseignements personnels.

Bien entendu, les normes en matière d'assurance qualité ne peuvent pas être considérées comme des substituts de la loi qui est essentielle pour l'établissement des directives d'ordre général que les organisations doivent respecter. Cependant, lorsque les règles juridiques sont établies en matière de protection de la vie privée (comme elles le sont effectivement dans la majorité des pays industrialisés), la tâche la plus importante consiste à s'assurer que les politiques établies visant la protection des données ou de la vie privée sont mises en œuvre au sein d'une organisation donnée. Un processus d'enregistrement aux fins de conformité à des normes, dans le cadre duquel les organisations doivent dire ce qu'elles font et faire en sorte que leurs pratiques fassent l'objet d'une vérification pour déterminer si leurs actes reflètent leurs paroles, pourrait éventuellement devenir l'un des différents « instruments stratégiques » des responsables de la protection des données.

vacy standards internationally and whether such instruments were indeed being properly implemented. Much of this analysis occurred as a result of the "adequacy" test under the 1995 EU Data Protection Directive. It is reasonably straightforward to compare the "black letter of the law" to determine whether legal provisions were indeed equivalent. It is also possible to compare the roles and responsibilities of supervisory authorities to determine the extent of independent oversight. Obviously, it was far more difficult to measure and compare actual compliance and thus give consumers real assurances that personal data transferred internationally were being afforded adequate levels of protection. Global electronic commerce increased the urgency of grappling seriously and internationally with the fundamental question: how were data protection authorities going to evaluate whether data protection rules were indeed being followed within other jurisdictions, especially when many of them lacked serious audit powers and methodologies?[15]

Second, the early attempts to address this concern did not inspire much confidence. There are, in fact, a variety of poorly defined and understood self regulatory instruments: privacy commitments about how an organization believes it treats personal information; privacy codes of practice which embody a codified set of rules for employees; privacy standards which imply not only a common yardstick for measurement, but also a process through which conformity to these norms might be assessed; and privacy seals – the 'good housekeeping' stamps of approval which give the organization that mark, symbol or cachet of privacy compliance. Ideally, the self regulatory process should be cumulative. An organization should declare its commitment to personal privacy protection, codify its policy, seek external certification for its practices, and then receive the seal of approval. [16]

In reality, the process of adopting these instruments is rarely a linear one. More often that not, public claims are made – especially on websites – without systematic internal analysis. Often "privacy policies" are not carefully codified. Frequently, privacy seals have been awarded without the kind of systematic and rigorous investigation and auditing characteristic of quality assurance programs.

Many companies were very keen to demonstrate their privacy-friendliness when the Internet be-

III. Justifications pour une norme de gestion de la vie privée

La plupart des mises en œuvre visant la protection des données concernent la transparence – à l'interne, vis-à-vis des membres de la direction et du personnel, et à l'externe, vis-à-vis des responsables des données et des organismes de réglementation. Dans les années 1990, un certain nombre d'experts de la protection des données et de la vie privée ont réalisé que le recours à une norme internationale en matière d'assurance qualité pourrait résoudre le problème de taille que pose la détermination des enjeux actuels relativement aux renseignements personnels que détiennent les organisations complexes. Les experts reconnaissent également que si la vie privée demeure un droit fondamental, il s'agit également d'un droit qui nécessite une mise en œuvre au sein d'organisations complexes.

Ainsi, en fonction des principes équitables en matière de renseignements[14], les normes de gestion permettent :

- de promouvoir la transparence des politiques de l'organisation et de ses buts;
- d'améliorer les procédures et de faire la vérification des données (règlement des plaintes, demandes d'accès et consentement);
- d'améliorer les procédures internes relatives à la gestion des renseignements personnels et d'en faire la vérification (sécurité, qualité et conservation des données).

Plusieurs facteurs expliquent pourquoi les experts songent à la possibilité de se servir des normes comme instrument faisant partie de la trousse de protection de la vie privée.

Premièrement, on reconnaît aisément que les préoccupations du consommateur en ce qui concerne la protection de la vie privée et la sécurité devaient être prises en compte au moment de la conception et de l'intégration du commerce électronique mondial, vers le milieu ou la fin des années 1990. Cette reconnaissance a mis en relief les difficultés éprouvées pour déterminer la comparabilité des normes de protection de la vie privée, à l'échelle internationale et pour savoir si de tels instruments avaient été mis en œuvre de façon adéquate. Une grande partie de cette analyse a été réalisée à la

came a powerful and widespread tool for electronic commerce. This enthusiasm resulted in a mad rush to develop and implement privacy seal programs which generally did not satisfy international regulators.[17] Further, there has been a proliferation of private sector privacy auditors, consultants, etc., who are not necessarily investigating and auditing to the same rigorous standards.

A third motivator for using a privacy management standard as part the privacy policy toolkit was a trend towards government outsourcing of personal data. This practice was creating situations where contractors were not being held to the same privacy standards as government agencies. Outsourcing has been a trend in many countries, especially in North America, although the contracted organizations have been all over the world. On other continents, contracts refer to standards and thus relieve government agencies of having to perform direct oversight of a contractor's operations. A condition of doing business with the government in some locations, therefore, is an ongoing registration to a particular standards program.[18] Even though there will be concerns that registration to a standard should not reduce government's regulatory responsibilities, nor relax privacy standards, there is an obvious potential for data protection authorities to use the standards registration process to ensure compliance when personal data is transmitted to an entity not otherwise covered by privacy protection law.

Any international privacy management standard should therefore entail:

- translating the existing fair information principles for processing personal data into standards language and format;
- separate guidance on how the principles should be implemented in organizations;
- conformity assessment tools, appropriate to the size of business and the sensitivity of the personal data processed;
- an audit guide; and
- a system for the accreditation of privacy auditors.

Hypothetically, there might be a number of ways in which a management standard for privacy might circulate around the global information economy.

suite des résultats obtenus pour un « test de pertinence » en vertu de la directive de 1995 de l'Union européenne relativement à la protection des données. Il est possible d'effectuer une comparaison assez honnête avec la « règle de droit immuable » pour déterminer si les dispositions légales sont effectivement équivalentes. Il est également possible de comparer les rôles et les responsabilités des organes de supervision pour déterminer la portée de la surveillance indépendante. Évidemment, il s'est avéré bien plus difficile d'évaluer et de comparer la conformité réelle et ainsi de garantir aux consommateurs que les renseignements personnels transmis à l'étranger seraient protégés, à un degré suffisant. Le commerce électronique mondial a fait en sorte qu'il devenant urgent de répondre sérieusement, à l'échelle internationale, à une question fondamentale : comment les autorités de protection des données allaient-elles faire pour évaluer si les règles de protection des données devaient être suivies par d'autres juridictions, plus particulièrement quand plusieurs d'entre elles ne disposaient pas de suffisamment de pouvoirs pour effectuer les vérifications et quand elles faisaient preuve d'un manque de méthode[15]?

Deuxièmement, les premières tentatives pour prendre en compte ces préoccupations n'ont pas vraiment inspiré confiance. Il existait, en réalité, une gamme d'instruments d'autorégulation mal définis et mal interprétés : engagements en matière de protection de la vie privée sur la façon dont une organisation estimait traiter les renseignements personnels; codes de pratique en matière de protection de la vie privée, qui se composaient d'un ensemble de règles codifiées à l'intention des employés; normes de protection de la vie privée, qui supposaient non seulement un critère commun pour l'évaluation, mais également un processus grâce auquel la conformité pouvait être évaluée; et des sceaux de confidentialité – en guise d'approbation – et l'organisation pouvait afficher cette marque, ce symbole ou ce sceau témoignant du respect de la vie privée. Idéalement, le processus d'autorégulation devait être progressif. Une organisation devait énoncer ses engagements en matière de protection de la vie privée, établir ses politiques, chercher à obtenir, de la part d'un organisme externe, une attestation de ses pratiques et recevoir ensuite le sceau d'approbation[16].

En réalité, le processus visant l'adoption de ces

Use of Educational and Regulatory Powers of Data Protection Authorities

Data protection authorities could use their discretion and influence in a number ways in order to increase the practice of organizations registering to a privacy standard (either a future international standard or, in Canada, the existing CSA standard), including:

- Publicly urging companies or sectors "at risk" to register. This could be particularly effective if timed to follow a public breach which, although perpetrated by one organization, has damaged the reputation of the entire sector;
- Obtaining the organization's agreement to seek registration during the mediation process, as a way for the organization to avoid the matter proceeding to an Inquiry;
- Using their authority to order an organization to register, should there be sufficient justification in their formal finding and the seriousness and breadth of noncompliance; and
- In the final instance, court-ordered registration in lieu of, or in addition to, a fine or other criminal penalties.[19]

Privacy Standards for Competitive Advantage

The greater the disparity between registered and unregistered organizations, the greater the perceived competitive advantage of being registered to a standard. Therefore, registered organizations are likely to publicize the fact in order to distinguish themselves, and will wear that registration as a badge of honour. This could take the form of organizations highlighting their registration in advertising, in corporate information and on websites, as they do with other such socially-responsible activities as recycling, adhering to fair trade practices and giving to the local community. When the "good privacy players" are seen to have registered, the value of the standard increases.

An organization's desire to distance itself from other players in a sector that has experienced a privacy breach could serve as a powerful incentive to register, and to publicize this fact. The closer an organization is to meeting the standards and regulations of its home jurisdiction, or those where it does business, the more likely it is to seek registration. In other words, those with good

instruments constitue rarement un parcours linéaire. La plupart du temps, les demandes du public – plus particulièrement celles faites par le biais d'un site Internet – ne font pas l'objet d'une analyse systématique à l'interne. Les « politiques relatives à la protection de la vie privée » sont souvent formulées avec nonchalance, peu soigneusement. Les sceaux de confidentialité sont souvent attribués sans la réalisation d'une vérification ou d'une enquête systématique et méthodique propre aux programmes d'assurance qualité.

Plusieurs entreprises étaient très enthousiastes et ont fait preuve d'ouverture en ce qui concerne la protection de la vie privée au moment où Internet est devenu un outil puissant et ubiquiste pour le commerce électronique. Cet enthousiasme s'est traduit par une course effrénée visant l'élaboration et la mise en œuvre de programme de sceaux de confidentialité qui ne donnaient pas satisfaction aux organismes internationaux de réglementation[17]. Par ailleurs, dans le secteur privé, le nombre de vérificateurs, de consultants etc., qui s'intéressaient à la protection de la vie privée s'est multiplié et ceux-ci n'effectuaient pas nécessairement une enquête ou une vérification de ces mêmes normes rigoureuses.

Un troisième facteur motive le recours à une norme de gestion de la protection de la vie privée qui pourrait faire partie d'un ensemble de politiques visant la protection des données : le gouvernement a tendance à impartir les renseignements personnels. Cette pratique engendre des situations où les entrepreneurs ne sont pas tenus de respecter les mêmes normes de protection de la vie privée que les agences gouvernementales. Le recours à l'impartition (ou à des ressources externes) est une tendance observée dans plusieurs pays, particulièrement en Amérique du Nord, et les organisations auxquelles les gouvernements font appel peuvent se trouver n'importe où sur la planète. Sur d'autres continents, les contrats font référence aux normes de sorte que les agences gouvernementales n'ont pas à exercer une surveillance directe des opérations ou des activités de l'entrepreneur. Dans certains pays, l'une des conditions pour qu'une organisation puisse faire affaire avec le gouvernement consiste en l'obligation d'un enregistrement en règle à un programme particulier de normes[18]. Malgré les préoccupations relativement au fait que l'enregistrement à une norme ne devrait avoir aucune incidence sur les

privacy practices are more likely to become registered in order to demonstrate that they are good privacy corporate players.

For organizations doing business internationally, particularly with jurisdictions whose level of privacy regulation is more stringent than its home jurisdiction, the organization could seek to distinguish itself from local competition by registering to a privacy standard. The benefits of this would be best felt if the standard were international.

Referencing the Standard in Contracts

Contracts can require the contractor to demonstrate registration to a recognized standard as a way to avoid stipulating certain practices or quality in detail. While both public and private sector organizations have often referenced standards in procurement documents, the onus is on the contract manager to audit to ensure adherence to standards. However, when an organization is registered to the standard, there is independent corroboration[20], and risks are decreased for the contracting party.

Referencing an international standard further decreases the risk when contracts are made between or among organizations with different jurisdictional bases which may have different national norms (the case with privacy). European organizations would be able to demonstrate due diligence in contracting out processes involving personal information when requiring the contractor to be registered to an international privacy standard that incorporated the EU rules. This takes the guesswork out of the business of determining adequate protection.

As with governments and businesses seeking to contract within or outside of their countries, research-funding organizations may require applicants to register to a standard. In Canada, organizations such as the Medical Research Council, the Social Sciences and Humanities Research Council and the Natural Sciences and Engineering Councils could require universities or other research institutions to register to the CSA privacy standard as a condition for receiving funding. In this way, the councils could ensure that the organization using their funds adhered to the same ethical standards for the treatment of personal information, without having to conduct checks on

responsabilités du gouvernement à titre d'autorité de réglementation, ni se traduire par des normes moins strictes en matière de protection de la vie privée, il est évident que les autorités de protection des données ont la possibilité d'avoir recours à un processus d'enregistrement à une norme pour assurer la conformité lorsque les renseignements personnels sont transmis à une entité qui ne serait pas autrement visée par la loi portant sur la protection de la vie privée.

Toute norme internationale de gestion de la protection de la vie privée doit par conséquent exiger :

- la traduction des principes d'équité existants en matière d'information, dans un format et un langage applicable aux normes;
- des directives distinctes portant sur la façon dont les principes doivent être mis en œuvre au sein des organisations;
- des outils d'évaluation de la conformité, en fonction de la taille de l'entreprise et de la nature délicate des données personnelles traitées;
- un guide de vérification;
- un système pour l'accréditation des vérificateurs œuvrant dans le domaine de la protection de la vie privée.

Hypothétiquement, il existe peut-être un certain nombre de mécanismes grâce auxquels une norme de gestion de la protection de la vie privée gagnerait à se faire connaître au sein du secteur mondial de l'information.

Recours aux pouvoirs de sensibilisation et de réglementation des autorités de protection des données

Les autorités de protection des données pourraient se servir de leur pouvoir discrétionnaire et exercer certaines influences dans le but d'améliorer les pratiques des organisations qui souscrivent au respect des normes de protection de la vie privée (qu'il s'agisse d'une norme internationale à définir ou, au Canada, de la norme CSA), y compris :

- encourager ou stimuler publiquement les entreprises ou les secteurs « plus à risque » à s'enregistrer en vue de se conformer à une norme. Cette mesure pourrait être particulièrement efficace si elle était recommandée à la suite d'une atteinte à la vie

each organization or wade through documentation to determine if their standards were met.

IV. The History of Privacy Management Standardization

Four main standards bodies have been involved over the last 10 to 15 years in attempts to develop an information privacy protection standard: the Canadian Standards Association (CSA), the International Organization for Standardization (ISO), the European Committee for Standardization/ Information Society Standardization System (CEN/ISSS) and the International Security, Trust and Privacy Alliance (ISTPA).

The Canadian Standards Association

Many national standards associations have embarked on standards initiatives with close connections to, and implications for, privacy and data protection. [21] Only one, however, has constructed a general management standard embracing the entire set of information privacy principles, and applying to all organizations. Work on a "privacy code" within a Technical Committee of the CSA began in 1993. Negotiations were time-consuming, but on September 20th, 1995, the Model Code for the Protection of Personal Information (Model Code) was passed. It was subsequently approved as a national standard of Canada (Q830) by the Standards Council of Canada in March 1996.

CSA's Model Code is constructed around 10 principles, each of which is accompanied by an interpretive commentary. Organizations and trade associations were expected to incorporate all principles in their entirety in their codes of practice and apply them to specific sectoral conditions. The Model Code was accompanied by a Workbook giving more practical advice and interpretation. At the time, some envisaged that the CSA Model Code would spread throughout the Canadian economy as a result of market pressures, moral suasion, contractual obligations and a general sense within Canadian business that this was a necessary way to avoid government regulation.

Although the Model Code uses certain prescriptive language such as "shall" and "must", it was designed as a voluntary instrument in the sense that organizations were not compelled to adopt it. Once adopted by an organization, however, the Model Code was designed to operate like any

privée au sein d'une seule organisation, mais ayant entaché la réputation de l'ensemble d'un secteur;
- l'obtention de l'approbation de la part d'une organisation pour que cette dernière cherche à s'enregistrer pendant le processus de médiation, une voie qu'une organisation peut emprunter pour éviter des poursuites à la suite d'une enquête;
- le recours à leurs pouvoirs pour exiger qu'une organisation s'enregistre si les résultats officiels le justifient et selon la gravité et la portée de la non-conformité;
- en dernière instance, l'enregistrement ordonné par la cour, plutôt qu'une sanction pénale (ou en plus d'une telle sanction ou de toute autre sanction pénale)[19].

Normes de protection de la vie privée et avantages concurrentiels

Plus les différences sont grandes entre les organisations enregistrées et celles qui ne le sont pas, plus les avantages concurrentiels de l'enregistrement à une norme se concrétisent. Par conséquent, les organisations sont plus susceptibles de faire connaître publiquement ce fait dans le but de se distinguer des autres et ainsi afficher cet enregistrement sur un tableau d'honneur. Pour ce faire, les organisations pourraient souligner leur enregistrement dans une publicité, dans un dépliant corporatif et sur leurs sites Internet respectifs, comme elles le feraient pour d'autres activités de responsabilisation sociale telles que le recyclage, les pratiques commerciales loyales et les dons faits auprès de la communauté locale. Quand des organismes sensibles à la protection de la vie privée sont perçus comme étant enregistrés, la valeur de la norme augmente.

Le désir d'une organisation de devancer ses concurrents sectoriels qui ont connu des problèmes liés à l'atteinte de la vie privée pourrait représenter un incitatif pour s'enregistrer et pour faire connaître cet engagement à respecter une norme. Plus une organisation cherche à satisfaire les normes et à respecter ses propres règlements – ou des juridictions où elle mène ses opérations – plus elle cherchera à s'enregistrer. Autrement dit, les organisations qui mettent en application de bonnes pratiques en matière de protection de la vie privée sont plus susceptibles de s'enregistrer dans le but de témoigner de leurs engagements relatifs à la protection de la vie

other standard. Claims of adoption would carry obligations: organizations would have to say what they do and do what they say. Accordingly, in 1996, the Quality Management Institute (QMI) announced a recognition program designed to allow businesses to register to the Model Code and thus demonstrate their compliance. This recognition program was sensitive to the fact that the privacy obligations of a large bank, insurance company and direct marketing firm were different from those of smaller or local enterprises. [22] Thus, unlike other self-regulatory instruments such as the OECD guidelines[23], QMI clearly specified what it meant to "adopt" the Model Code. Businesses would have to develop an internal code of practice consistent with the Code, produce a set of guidelines for its internal implementation, and then apply to an accredited registrar to achieve a registration. Like other standards, the CSA's Model Code was intended for registration, and to motivate some consistency in the marketplace and a higher level of consumer confidence.

The implementation of this Model Code was never fully realized because the Canadian government decided to develop private sector privacy legislation in 1999. *The Protection of Personal Information Protection and Electronic Documents Act* (PIPEDA) began its phased application in 2001. The central purpose of the legislation was to require organizations engaged in commercial activity in Canada to comply with the Model Code, reproduced verbatim in its Schedule 1. Thus, what had begun as an innovative self-regulatory measure was overtaken by political and legislative pressures. Transforming the code from a standard to law increased the breadth of its application but made compliance reactive rather than proactive, as it would have been for companies registering to the standard.

There were explicit reasons why the drafters of PIPEDA decided to legislate by reference to CSA's Model Code. First, they believed that, since the private sector had already negotiated this standard, the legislation would do nothing more than force companies to "live up to their own rules". Secondly – and this point has been lost – the CSA Model Code in itself was seen as a crucial mechanism for ensuring compliance which could augment the federal Privacy Commissioner's modest compliance resources. If an organization were registered, the Model Code would cease to be a "voluntary" mechanism. That organization would have to produce a code and a

privée.

Pour les organisations qui transigent au niveau international, plus particulièrement avec des juridictions dont la réglementation en matière de protection de la vie privée est plus sévère ou plus stricte que dans leurs pays d'origine, celles-ci devraient chercher à se distinguer des autres, incluant leurs concurrents locaux, en s'enregistrant en vue se conformer à une norme visant la protection de la vie privée. Les avantages qui pourraient en résulter seraient plus importants si la norme était reconnue à l'échelle internationale.

Référence à une norme dans les contrats

Les contrats peuvent stipuler que l'entrepreneur doit prouver qu'il est enregistré en vue de se conformer à une norme reconnue : il s'agit d'un moyen pour éviter de préciser certaines pratiques ou d'apporter des détails à certains points touchant la qualité. Si les organisations relevant du secteur public ou privé ont souvent fait référence à des normes dans les devis, le gestionnaire du contrat porte le fardeau de la vérification pour s'assurer du respect des normes. Cependant, lorsqu'une organisation est enregistrée pour se conformer à une norme, la corroboration est effectuée par une organisation indépendante[20], et la partie contractante court alors moins de risques.

En faisant référence à une norme internationale, les risques sont atténués lorsque les contrats sont établis entre des organisations et des juridictions différentes qui pourraient être dans l'obligation de satisfaire à différentes normes nationales (comme c'est le cas avec la protection de la vie privée). Les organisations européennes doivent être en mesure de faire preuve de diligence raisonnable en matière d'impartition des processus liés à la protection des renseignements personnels lorsqu'un entrepreneur doit s'enregistrer en vue de se conformer à une norme internationale de protection de la vie privée qui intègre la réglementation de l'Union européenne. L'entreprise quitte alors le domaine de la conjecture pour déterminer si la protection est adéquate.

Comme pour les gouvernements et les entreprises qui cherchent à établir des contrats à l'intérieur du pays ou à l'étranger, les organisations de subventions de recherche

related set of operational guidelines and be subjected to regular and independent auditing of its practices by an accredited registrar. A Commissioner, in sanctioning an organization for a well-founded complaint, could not only assess a fine, but also require the organization to change its practices – and to demonstrate that it had – by registration to the privacy standard. Conversely, the demonstration that a code of practice is indeed complied with throughout the organization should have powerful evidentiary force. This should not exempt the organization from the provisions of PIPEDA, but it should carry weight in any investigations by, or proceedings before, the Commissioner or the courts.

Furthermore, registration to the CSA Model Code would assist in the interpretation and enforcement of Principle 4.1.3 which requires organizations to "use contractual or other means to provide a comparable level of protection while the information is being processed by a third party". It could also assist with the tricky question of how to assure comparable levels of protection when a Canadian company outsources personal data processing to an overseas organization. Contracts could reference the standard; registration to the standard would be a condition for continual processing of Canadian personal data.

Has the need to become certified been made redundant by the code's inclusion in PIPEDA? Why would organizations go to the time and expense of demonstrating compliance through registration when they are already required by law to comply?

According to the Commissioner's 2006 Annual Report on PIPEDA, of 424 complaints, only 21 per cent were "not well founded", an indication that organizations' compliance with the legislation is underwhelming.[24]

Further studies have found that many organizations are unaware of their obligations, and that stated privacy policies are misleading and incomplete.[25] Many organizations that are aware of the law simply wait for a complaint to be made, knowing that they can demonstrate willingness during investigation and mediation and escape without penalties. Other companies may not consciously see themselves taking a business risk but merely hold off making any changes in their personal information practices, waiting to see what individuals object to. It appears that the pro-

peuvent exiger d'être enregistré à une norme. Au Canada, des organisations telles que l'Institut de recherche en santé du Canada, le Conseil de recherches en sciences humaines et le Conseil de recherches en sciences naturelles et en génie pourraient demander aux universités, ou à d'autres institutions dédiées à la recherche, de s'enregistrer en vue de se conformer aux normes CSA relativement à la protection de la vie privée, à titre de condition préalable pour l'octroi de financement. De cette façon, ces institutions s'assureraient que l'organisation qui utilise les fonds adhère aux mêmes normes éthiques en matière de traitement des renseignements personnels, sans avoir à effectuer les vérifications pour chacune des organisations ni à parcourir toute la documentation pour savoir si les normes ont été satisfaites.

IV. Historique de la normalisation de la gestion de la protection de la vie privée

Quatre principaux organismes rédacteurs de normes ont cherché, au cours des dix ou quinze dernières années, à élaborer une norme de protection des données et de la vie privée : l'Association canadienne de normalisation (CSA), l'Organisation internationale de normalisation (ISO), le Système de normalisation de la société de l'information du Comité européen de normalisation (CEN-ISSS) et le International Security, Trust, and Privacy Alliance (ISTPA).

Association canadienne de normalisation (CSA)

Plusieurs associations nationales de normalisation ont participé à des initiatives d'élaboration de normes étroitement liées aux enjeux de la protection des données et de la vie privée – ou qui pouvaient avoir des incidences sur ces enjeux[21]. Cependant, une seule association a mis au point une norme de gestion d'ordre général qui englobe un ensemble de principes de protection des données et de la vie privée, et qui s'applique à toutes les organisations. Les travaux portant sur un « code de protection de la vie privée » ont été entamés en 1993 par un comité technique de la CSA. Les négociations prenaient du temps mais, le 20 septembre 1995, le Code type sur la protection des renseignements personnels était adopté. Ce dernier a par la suite été approuvé à titre de norme nationale du Canada (Q830) par le Conseil canadien des normes (CCN) en mars 1996.

active CSA Standard, in becoming law, has become a more reactive instrument.

The International Standardization Organization (ISO)

By the late 1990s, observers were calling for Canada's national standard, the CSA Model Code, to become internationalized, and there was pressure on ISO to take up the issue. Privacy protection laws were proliferating around the world and regulations were "trading up" as countries and regions were trying to establish competitive advantages in electronic commerce. Companies were also looking for ways to simplify and improve confidence in their sub-contracting and contracting out processes concerning the treatment of personal information.

Many felt that a separate ISO privacy standard would be in the interests of all nations and stakeholders. It would carry far greater weight and credibility worldwide, therefore benefiting more people and organizations. It would attract attention and international registration efforts from different national standards bodies, and would create a market for more specialized compliance tools. And it would give businesses in countries which have not been deemed "adequate" under European data protection law a more reliable and consistent method of demonstrating their conformity to international data protection standards.[26] In May 1994, ISO's consumer associations' committee (COPOLCO) established a working group to determine whether the then-draft standard of the Canadian Standards Association could form the basis of an international standard for protecting personal data. The Group recommended to COPOLCO in April 1996 that ISO develop an international standard. ISO's General Council accepted this recommendation in September 1996 and resolved that rapid advances in technology and the growth of electronic communication and databases demanded global rules for the protection of personal information. It noted that, while regulations differ throughout the world, consensus based standards could help provide a global base of protection. The ISO General Council also asked the Secretary-General to refer the COPOLCO recommendation to the Technical Management Board (TMB) for appropriate action, together with the comments made during the meeting. In determining how work would begin on this standardization effort, ISO's twelve-member

Le Code type de la CSA a été élaboré en fonction de dix principes, chacun d'eux faisant l'objet d'un commentaire sur l'interprétation. Il était prévu que les organisations et les associations commerciales adopteraient tous les principes intégralement dans leurs codes de pratique et qu'elles les mettraient en application dans des situations particulières à chaque secteur. Le Code type était accompagné d'un guide comprenant des conseils pratiques et des points de repère pour l'interprétation. En même temps, certains pensaient que le Code type de la CSA s'étendrait à l'économie canadienne en raison des pressions boursières, de la persuasion, des obligations contractuelles ainsi qu'en raison d'un sentiment partagé par les entreprises canadiennes qui estimaient que le Code type était nécessaire pour éviter une réglementation émanant du gouvernement.

Bien que le Code type ait recours à un certain langage prescriptif et conjugue le verbe « devoir », il a été élaboré à titre d'instrument volontaire, c'est-à-dire, que les organisations n'étaient pas obligées de l'adopter. Toutefois, lorsqu'une organisation adoptait un tel instrument, le Code type était élaboré pour être appliqué comme n'importe quelle autre norme. Toute adoption officielle suppose des obligations : les organisations doivent expliciter ce qu'elles font et faire ce qu'elles disent. Par conséquent, en 1996, le Quality Management Institute a annoncé qu'un programme de reconnaissance avait été élaboré pour permettre aux entreprises d'adopter le Code type et prouver ainsi qu'elles s'y conformaient. Ce programme de reconnaissance tenait compte du fait que, relativement à la protection de la vie privée, les obligations d'une importante banque, d'une compagnie d'assurances et d'une firme de marketing direct différaient de celles d'entreprises de plus petite taille ou d'entreprises locales[22]. Ainsi, à la différence d'autres instruments d'autorégulation tels que les lignes directrices de l'OCDE[23], le QMI a clairement indiqué l'adoption du Code type. Les entreprises devaient élaborer un code de pratique interne, conforme au Code, et rédiger un ensemble de lignes directrices en vue de leur mise en œuvre pour ensuite faire une demande auprès d'un registraire accrédité pour compléter le processus d'enregistrement. Tout comme pour les autres normes, le Code type de la CSA visait l'enregistrement aux fins de conformité et voulait encourager une certaine cohérence dans le marché et augmenter le degré de confiance des consommateurs.

TMB decided to refer the issue to an ad hoc advisory group (AHAG) in January 1997. The AHAG was supposed to produce a positive TMB resolution in 1998. However, reservations about this initiative from representatives of the American National Standards Institute (ANSI) had already been circulated, and the expected resolution did not materialize. The AHAG continued to study the issue for another year but was disbanded in June, 1999. A meeting in Hong Kong later that year concluded that some other useful standardization instruments, short of a full-fledged privacy standard, could be negotiated but that a general management standard should be laid "dormant". It recognized that the work was being taken up by the European Committee for Standardization (CEN) and was prepared to take up the issue again if requested.

Privacy protection does, however, intersect with standards development in other sectors. A few examples include: Financial Services (TC 680); Road Transport Informatics (TC 204); Geographic Information and Geomatics (TC 211); and Health Informatics (TC 215). Also, there is now a family of standards on IT security within an ISO 27000 series.[27] ISO 27002 is the generic code of practice for IT security, itself based on the original British standard, BS 7799. Most notably, privacy-related work has been independently pursued by a joint technical committee (JTC-1) of the ISO and International Electro-Technical. This joint committee has been building various base standards in the field of information and communications technology, some of which have key privacy components.[28]

There are a number of technical committees within JTC-I of which Subcommittee 27 is the lead on IT security. SC 27 has the task of standardizing "generic IT security services and techniques". This includes identifying generic requirements (including requirements methodology) for IT system security services; developing security techniques and mechanisms (including registration procedures and relationships of security components); developing security guidelines (e.g., interpretative documents, risk analysis); developing management support documentation and standards (e.g. terminology and security evaluation criteria); and standardizing cryptographic algorithms for integrity, authentication and non-repudiation services.[29] Within SC-27 there are five working groups, the most recent of which is Working Group No. 5,

La mise en œuvre du Code type n'a jamais été réalisée dans sa totalité parce qu'en 1999, le gouvernement du Canada a décidé d'élaborer des lois sur la protection de la vie privée s'appliquant au secteur privé. La mise en application graduelle de la *Loi sur la protection des renseignements personnels et les documents électroniques* (*LPRPDÉ*) a débuté en 2001. Le principal but de la loi est de demander aux organisations qui se consacrent à des activités commerciales au Canada de se conformer au Code type, reproduit tel quel dans l'annexe 1 de la Loi. Ainsi, une mesure d'autorégulation novatrice a été reprise en raison des pressions politiques et législatives. Le code est alors devenu une norme transformée en loi et cette modification a élargi la portée de son application, malgré que les organisations se conforment par une approche réactive plutôt que par une gestion proactive, comme c'est le cas pour les entreprises qui désirent s'enregistrer en vue de se conformer à une norme.

Des raisons expliquent pourquoi les rédacteurs de l'ébauche de la *LPRPDÉ* ont décidé d'établir la législation en faisant référence au Code type de la CSA. Premièrement, ils croyaient que, puisque le secteur privé avait déjà pris des arrangements pour se conformer à cette norme, la loi ne ferait rien d'autre que d'obliger les entreprises à « respecter leurs propres règles ». Deuxièmement – et ce point a été perdu de vue – le Code type de la CSA en lui-même était perçu comme étant un mécanisme essentiel pour garantir la conformité, ce qui aurait pu augmenter le nombre de modestes ressources du Commissariat à la protection de la vie privée du Canada en matière de conformité. Si une organisation était enregistrée, le Code type ne serait plus un instrument dit « volontaire ». Cette organisation se verrait alors dans l'obligation d'élaborer un code ainsi qu'un ensemble connexe de directives opérationnelles et de se plier à des vérifications indépendantes et régulières de ses pratiques par un registraire accrédité. Lorsqu'il sanctionne une organisation pour une plainte fondée, un commissaire doit non seulement évaluer une organisation en règle, mais doit également exiger que l'organisation modifie ses pratiques – et qu'elle prouve qu'elle l'a fait – en s'enregistrant en vue de se conformer à une norme de protection de la vie privée. Démontrer qu'un code de pratique est appliqué dans l'ensemble de l'organisation devrait constituer une preuve convaincante. Cette démarche ne devrait pas avoir pour effet d'exempter l'organisation des

responsible for Identity Management (IdM) and Privacy Technologies. Its remit includes developing and maintaining standards and guidelines to address security aspects of identity management, biometrics and the protection of personal data.[30] The following initiatives are currently being undertaken:

- A Framework for Identity Management (ISO/ IEC 24760)
- A Privacy Framework (ISO/IEC 29100)
- A Privacy Reference Architecture (ISO IEC 29101)
- An Authentication Context for Biometrics (ISO/ IEC 24761)
- A Biometric Template Protection (ISO/IEC 24745)

The first two seem to be the most advanced. The Framework for Identity Management is designed to provide a framework for the secure and reliable management of identities online with appropriate definitions, concepts and models. It describes the basic components of IdM and the life cycle of identities as they are established, modified, suspended and archived. This standard is designed to form the basis of future ISO identity standards and is currently at the level of a working draft.

ISO/IEC 29100 provides a more general privacy framework. It provides common privacy terminology and defines the basic privacy principles. It is also designed to relate privacy requirements to existing security standards and guidelines, and particularly those within the ISO 27000 series. On the face of it, ISO 29100 appears to be intended as a general privacy standard of similar breadth and applicability to that contemplated in the late 1990s. But it is also obvious that the principal motivation is the need to address online privacy risks. This proposed standard is accompanied by ISO/IEC 29101 designed to standardize best practices for the consistent technical implementation of personal information privacy requirements, the assumption being that the privacy framework should be established before the architecture.

It is premature to conclude which of these initiatives will materialize into full ISO standards. What is apparent is that distinctions between technical and management standards tend to be breaking down, that privacy protection principles are embedded in the work of ISO at many

dispositions de la *LPRPDÉ*, mais, dans le cadre de toute enquête ou de toute procédure devant le commissaire et les tribunaux, elle devrait pouvoir être présentée en preuve.

Par ailleurs, l'inscription au Code type de la CSA doit faciliter l'interprétation et favoriser le respect du principe 4.1.3, qui stipule que « L'organisation doit, par voie contractuelle ou autre, fournir un degré comparable de protection aux renseignements qui sont en cours de traitement par une tierce partie ». Il serait également plus facile de répondre à cette question épineuse : comment garantir un degré comparable de protection alors que les entreprises canadiennes impartissent le traitement des renseignements personnels à des organisations à l'étranger? Les contrats doivent faire référence à la norme; l'enregistrement à la norme pourrait être une condition pour poursuivre les activités de traitement des renseignements personnels des Canadiennes et Canadiens.

La certification serait-elle devenue superflue en raison de l'intégration du code dans la *LPRPDÉ*? Pourquoi les organisations consacreraient-elles temps et argent pour prouver la conformité à la norme en s'enregistrant alors qu'elles sont obligées par la loi de s'y conformer?

Selon le rapport annuel de l'année 2006 de la commissaire à la protection de la vie privée portant sur la *LPRPDÉ*, sur 424 plaintes, seulement 21 p. 100 d'entre elles étaient non fondées, une indication que les organisations ne respectent pas toujours la loi[24].

D'autres études ont démontré que plusieurs organisations ne connaissent pas leurs obligations et que les énoncés de politique en matière de protection de la vie privée sont incomplets et induisent en erreur[25]. Plusieurs organisations, conscientes qu'il est toujours possible de déposer une plainte en vertu de la loi, savent qu'elles peuvent prouver leur bonne volonté en cours d'enquête et de médiation sans recevoir une sanction. D'autres entreprises peuvent ne pas être conscientes du fait qu'elles prennent des risques mais elles se contentent d'attendre pour apporter des changements dans les pratiques de protection des renseignements personnels pour voir ce qui pourrait être remis en question. Il semble que la norme CSA, plus proactive, ressemble davantage à un instrument de gestion réactive depuis qu'elle est devenue une loi.

different levels and in many different projects, and that the community of international privacy and data protection agencies need to be more adequately informed about, and involved in, the ISO standards development process.

The European Committee for Standardization/Information Society Standardization System (CEN/ISSS)

CEN, the European Committee for Standardization, was founded in 1961 by the national standards bodies in the European Economic Community and the European Free Trade Area countries.[31] CEN is now "contributing to the objectives of the European Union and European Economic Area with voluntary technical standards which promote free trade, the safety of workers and consumers, interoperability of networks, environmental protection, exploitation of research and development programmes, and public procurement".

CEN's involvement with privacy began through a multi-stakeholder group entitled the Initiative for Privacy Standardization in Europe (IPSE) which reported in 2002.[32] IPSE recommended that CEN/ ISSS should: identify a common European set of voluntary best practices for data protection; develop a generic set of contract clauses reflecting the requirements of Article 17 of the European Directive; prepare an inventory of data protection auditing practices; conduct a survey of web seal programs as a basis for considering further standardization; develop a coherent approach for assessing the impact of ongoing technological developments; and compile and deliver a targeted range of educational and guidance material on privacy-related standardization issues. IPSE did not, however, recommend a management standard at the European level, arguing that "there is no evident immediate industry demand at the European level for a management type standard for privacy". IPSE also suggested that "any work on a European management standard is premature at this time, and that individual European privacy interests have an avenue to pursue these objectives through the ISO route, building on the COPOLCO resolutions, if desired".[33] CEN's work has proceeded through a series of workshops of its Information Society Standardization System (ISSS), including the Data Protection and Privacy Workshop (CEN/ISSS/WS/DPP). The Workshop's

Organisation internationale de normalisation (ISO)

Vers la fin des années 1990, des observateurs désiraient que la norme nationale canadienne – le Code type de la CSA – devienne une norme internationale, et des pressions ont été exercées pour que l'ISO se penche sur le sujet. Les lois de protection de la vie privée se multipliaient dans tous les pays et les réglementations étaient plus strictes au fur et à mesure que des pays et certaines régions tentaient de profiter des avantages concurrentiels du commerce électronique. Les entreprises cherchaient également des moyens de simplifier et d'augmenter le degré de confiance envers les processus liés à la sous-traitance et à l'impartition relativement au traitement des renseignements personnels.

Plusieurs estimaient que l'établissement d'une norme ISO distincte en matière de protection de la vie privée serait profitable à toutes les nations et à tous les intervenants et dans leur plus grand intérêt. Elle pourrait avoir beaucoup plus de poids et de crédibilité à l'échelle internationale, et un plus grand nombre de personnes et d'organisations pourraient en tirer avantage. Elle attirerait l'attention et encouragerait les efforts en matière d'enregistrement à une norme internationale auprès de différents organismes nationaux de normalisation et entraînerait la création d'un marché pour des outils de conformité plus spécialisés. Ceci pourrait donner accès aux entreprises de pays qui ne sont pas jugés « adéquats » en vertu de la loi européenne de protection des données à une méthode plus fiable et cohérente pour prouver qu'elles respectent les normes internationales de protection des données[26]. En mai 1994, le Comité pour la politique en matière de consommation (COPOLCO) de l'Organisation internationale de normalisation (ISO) a constitué un groupe de travail pour déterminer si l'ébauche de la norme de la CSA pourrait servir d'assise pour une norme internationale de protection des renseignements personnels. En avril 1996, le groupe de travail recommandait au COPOLCO que l'ISO prépare une norme internationale. Le Conseil général de l'ISO approuva cette recommandation en septembre 1996 et statua que les avancées rapides de la technologie et l'évolution des communications électroniques et des bases de données informatiques supposaient des règles d'ordre international pour la protection des

aim is to "help organizations to comply with the Data Protection Directive and relevant national legislation by facilitating harmonization of practice, developing the understanding and predictability of detailed or sector practices, contributing to resolving ICT technical compliance issues, and encouraging consistency of assessment and oversight".[34]

The Workshop has already completed several reports in 2005 and 2006, including:

- an inventory of Data Protection Auditing Practices;
- an analysis of Privacy Protection Technologies, Privacy-Enhancing Technologies (PET), Privacy Management Systems (PMS) and Identity Management systems (IMS), the Drivers thereof and the need for standardization;
- a standard form contract to assist compliance with obligations imposed by article 17 of the Data Protection Directive 95/46/EC (and implementation guide);
- Personal Data Protection Audit Framework (EU Directive EC 95/46): Part I: Baseline Framework – The protection of Personal Data in the EU; and
- Personal Data Protection Audit Framework (EU Directive EC 95/46) Part II: Checklists, questionnaires and templates for users of the framework – The protection of Personal Data in the EU.[35]

In addition, the workshop participants have identified further work areas to be developed, with a focus on small and medium enterprises, on self-assessment and on a much closer dialogue between firms and regulators.

These further work areas are:

- a Common European set of voluntary best practices for data protection management to help businesses and data managers comply with the Directive and, where possible and appropriate, the diverse European national laws and additional requirements;
- EU privacy audit tools: towards a practical approach of audit tools for data managers, enabling them to perform self assessment; and
- a Voluntary Technology Dialogue System: ensuring new products, technologies and services comply with the relevant Data Protection and Privacy laws as transposed in

renseignements personnels. Il fit remarquer que, si les réglementations différaient à travers le monde, les normes élaborées ayant fait l'objet d'un consensus pouvant servir de base en matière de protection de la vie privée. Le Conseil général de l'ISO a également demandé au Secrétariat général de rappeler l'existence des recommandations du COPOLCO auprès du Bureau de gestion technique (BGT) pour prendre des mesures appropriées, ainsi que des commentaires formulés au cours de la réunion. Pour déterminer comment entamer le travail et orienter les efforts de normalisation, les douze membres du BGT de l'ISO ont décidé de poser cette question à un comité consultatif spécial en janvier 1997. Ce dernier devait faire en sorte que le BGT approuve la résolution en 1998. Cependant, les représentants de l'American National Standards Institute (ANSI) ont manifesté leurs réserves vis-à-vis de cette initiative qui avait déjà été émise et la résolution n'a pas été adoptée. Le comité consultatif spécial a étudié l'enjeu pendant une année supplémentaire mais il a été dissous en juin 1999. Lors d'une réunion tenue ultérieurement à Hong Kong cette année-là, on a conclu que les autres instruments de normalisation utiles – une norme visant le respect de la vie privée, en bonne et due forme – pouvaient faire l'objet de pourparlers mais que le projet d'établissement d'une norme de gestion d'ordre général devait être mis de côté. Il fut admis que le travail soit repris par le Comité européen de normalisation (CEN) qui était prêt à se pencher de nouveau sur le sujet, sur demande.

La protection de la vie privée est liée à l'élaboration de normes dans d'autres secteurs. Mentionnons quelques exemples : la norme relative aux services financiers (TC 680); informatique et transport routier (TC 204); information géographique et la géomatique (TC 211); informatique de la santé (TC 215). Il existe aussi actuellement un ensemble de normes sur la sécurité de la TI à l'intérieur des séries ISO 27000[27]. La norme ISO 27002 est un code de pratique générique pour la sécurité informatique, qui se fonde à son tour sur une norme britannique (BS 7799). Il faut surtout noter que le travail d'élaboration de normes de protection de la vie privée a été réalisé de façon indépendante pour un comité technique mixte (JTC 1) de l'ISO et de la Commission électrotechnique internationale (CEI). Ce comité mixte a préparé diverses normes de base dans le domaine de la technologie de l'information et des communications, et certaines

all EU member states can be a challenging task for industry.

In addition, regulators find themselves somewhat unaware of potential new technologies likely to reach the market in the near future.

The International Security, Trust and Privacy Alliance (ISTPA)

"ISTPA" is the International Security, Trust, and Privacy Alliance, founded in 1999. It is a "global alliance of companies, institutions and technology providers". Its self-proclaimed mission is to "clarify and resolve existing and evolving issues related to security, trust, and privacy". Further, it states that its "focus is on the protection of personal information".[36]

Its goals are to:

- Develop a Framework for the protection of personal and organizational data, which defines security, privacy, and trust services and their relationship.
- Develop an understanding of the usability, manageability and cost implications of technologies supporting data protection.
- Conduct research, demonstrations and inter-operability projects which address critical privacy, security, and trust issues.
- Provide guidance to member companies.
- Provide international forums for discussion of issues and solutions.
- Serve as a voice and resource for industry on privacy technology issues.
- Promote the ISTPA's work and its mission.

ISTPA's Privacy Framework 1.1 was intended primarily for an audience of privacy officers or those responsible for privacy within their organizations but also for legislators and government officials seeking to regulate.[37] ISTPA had developed the Framework as "a comprehensive and valuable aid for those implementing privacy policies in information systems containing personally identifiable information".38 It was also intended to help organizations deal with technical issues when grappling with privacy across jurisdictions. The Framework was subsequently submitted by the International System Security Engineering Association (ISSEA) as a candidate for an ISO Publicly Available Specification (PAS), 39and was

d'entre elles comprennent des éléments clés qui s'appliquent à la protection de la vie privée[28].

Il existe un certain nombre de comités techniques à l'intérieur du JTC 1, dont le sous-comité 27 (SC 27) qui se penche sur la sécurité informatique. Le SC 27 est chargé d'uniformiser les normes génériques des services et des techniques de sécurité informatique, ce qui comprend la détermination des exigences génériques (y compris la méthode d'établissement des exigences) pour les services de sécurité d'un système informatique; la conception de techniques et de mécanismes pour assurer la sécurité (y compris les procédures d'enregistrement et les relations entre les éléments en matière de sécurité), l'élaboration de lignes directrices portant sur la sécurité (c.-à-d., documents d'interprétation, analyse des risques); la production de document de soutien de la gestion et élaboration de normes (p. ex., terminologie et critères d'évaluation de la sécurité); et l'uniformisation des algorithmes cryptographiques pour l'intégrité, l'authentification et la non-répudiation des services[29]. Le SC 27 se compose de cinq groupes de travail, dont le plus récent est le groupe de travail n° 5, qui est responsable de la gestion de l'identité et des technologies de protection de la vie privée. Il a pour mandat l'élaboration et la mise à jour des normes et des lignes directrices pour traiter des aspects liés à la sécurité et à la gestion de l'identité, la biométrie et la protection des données personnelles[30]. Les initiatives énumérées ci-dessous sont actuellement en cours de réalisation pour la mise en place :

- d'un cadre pour la gestion de l'identité (ISO/ CEI 24760);
- d'un cadre de la protection de la vie privée (ISO/CEI 29100);
- d'une architecture de référence pour la protection de la vie privée (ISO/CEI 29101);
- d'un contexte d'authentification pour le recours à la biométrie (ISO/CEI 24761);
- d'un modèle de protection biométrique (ISO/ CEI 24745).

Les travaux des deux premières initiatives sont plus avancés. Le cadre pour la gestion de l'identité est conçu pour fournir un cadre de gestion sécuritaire et fiable des identités « en ligne », à l'aide des définitions, des concepts et des modèles appropriés. Il procure une description des éléments de base de la gestion de

also brought forward to the international data protection commissioners at their conference in Wroclaw, Poland in 2004.

Historically, data protection authorities have not been heavily involved with standards related activities. However, their Article 29 Working Group did issue an opinion on May 29, 1997, expressing its support for such initiatives as "significantly contributing to the protection of fundamental rights and privacy on a world-wide basis".40 In Wroclaw, the commissioners passed a resolution that "a global privacy standard(s) and specifically a privacy technology standard be developed by ISO that would support the implementation of legal rules on privacy and data protection where they exist and the formulation of such rules where they are still lacking". In doing so, the commissioners also expressed their concern that initiatives in ISTPA and JTC1 were producing privacy management frameworks which would be inconsistent with extant European data protection law. They went on to resolve that "developing an international privacy standard must be based on the fair information practices as well as the concepts of data scarcity, minimization and anonymity".41 ISTPA is re-writing the ISTPA Privacy Framework document to address the concerns raised by the International Conference, with the eventual goal of re-introducing the document for consideration as an ISO standard.

V. Conclusion: Implications for Data Protection Authorities

At the end of 2007, the landscape for privacy standardization features:

- A national privacy standard for Canada which has been rendered almost redundant by the passage of PIPEDA;
- Significant activity within the ISO JTC-1 towards negotiating base technical standards, some of which have key privacy components and implications; and
- A considerable amount of work within CEN/ ISSS on data protection audit and contracting processes, as well as on privacy-enhancing technologies. However, it is not yet clear how this work is being integrated into the day- to-day work of the data protection authorities, and less still into the practical data protection compliance of European companies.

l'identité et de leur cycle de vie au moment où celles-ci sont générées, modifiées, mises hors service et archivées. Cette norme est élaborée pour jeter les bases des futures normes ISO en matière d'identité; il s'agit actuellement d'une ébauche.

La norme ISO/CEI 29100 fournit un cadre de la protection de la vie privée d'ordre plus général. Elle permet de connaître la terminologie en matière de protection de la vie privée et en définit les principes de base. Elle a également été rédigée pour permettre d'établir un rapport entre, d'une part, les exigences relatives à la protection de la vie privée et, d'autre part, les normes et les lignes directrices existantes en matière de sécurité, et plus particulièrement celles qui font partie des séries ISO 27000. De prime abord, la norme ISO 29100 peut être assimilée à une norme de protection de la vie privée d'ordre plus général, de portée similaire et dont la mise en application est semblable à celles étudiées vers la fin des années 1990. Mais il est aussi évident que la principale raison justifiant l'élaboration d'une telle norme est la nécessité d'atténuer les risques liés à l'utilisation d'Internet en vue de protéger la vie privée. La norme proposée va de pair avec la norme ISO/CEI 29101 qui vise à uniformiser les pratiques exemplaires pour une mise en œuvre technique cohérente des exigences liées à la protection de la vie privée et des renseignements personnels, en posant pour hypothèse que le cadre de protection de la vie privée devrait être établi avant l'architecture.

Il est encore trop tôt pour prédire laquelle de ces initiatives se traduira par la mise en œuvre de normes ISO. Il est évident que les distinctions entre les normes techniques et les normes de gestion ont tendance à s'atténuer, que les principes de protection de la vie privée sont intégrés dans les normes ISO, à des degrés différents et dans plusieurs projets de différente nature et que la communauté des agences internationales de protection des données et de la vie privée doit être adéquatement informée concernant le processus d'élaboration de normes ISO et être appelée à y participer davantage.

Système de normalisation de la société de l'information du Comité européen de normalisation (CEN-ISSS)

Le Comité européen de normalisation (CEN) a été fondé en 1961 par les organismes nationaux de

The idea of a general management standard – an international version of the CSA Model Code – has been difficult to realize. This can be explained by:

- a certain reluctance by standards bodies to enter an area traditionally conceived in terms of human rights;
- a skepticism on the part of privacy advocates and regulators about the appropriateness of another set of international institutions becoming involved with this issue;
- a fear among advocates and regulators that a general management standard would undermine existing data protection law;
- in some areas, stiff opposition to the idea of a general management standard from certain private sector interests; and
- the proliferation of seal and certification schemes on the Internet, which have allowed companies to provide an illusion of privacy compliance without having to undertake a rigorous standards registration process.

One wonders then if a management standard for privacy protection is an idea whose time has passed. Yet, in contemporary circumstances, where data breaches are commonplace, the vision for a fully functioning standards system for privacy protection which can support existing law remains as valid as ever.

The process of attaining and maintaining registration to a privacy standard can relieve pressure on data protection agencies as the sole oversight authorities. In an environment of global personal data processing, the scrutiny of laws and contracts provides no assurances to data protection authorities that the receiving jurisdiction complies with data protection rules. Registration to a standard, which would oblige independent and regular auditing, would provide a greater certainty that the receiving organization practices "adequate" data protection, wherever it is located and whatever its business. Registration can also provide more meaningful guarantees for consumers looking to conduct business with privacy-friendly organizations – "meaningful" because an organization's adherence to good privacy practices has been independently verified, and also because, as a product of a standards authorities, its requirements are rigorous and harmonized.

Given that a stand-alone international privacy

normes qui font partie de la Communauté économique européenne et de la Zone européenne de libre-échange[31]. Le CEN « donne maintenant son apport pour l'atteinte des objectifs de l'Union européenne et de l'Espace économique européen, grâce aux normes techniques volontaires qui font la promotion du libre-échange, la sécurité des travailleurs et des consommateurs, l'interopérabilité des réseaux, la protection de l'environnement, le recours à des programmes de recherche et de développement et les marchés publics » [traduction].

Le CEN a d'abord participé aux réunions d'un groupe réunissant de multiples intervenants; ce groupe participait à un projet de normalisation de la protection de la vie privée en Europe (intitulé « Initiative for Privacy Standardization in Europe – IPSE) qui a produit un rapport en 2002[32]. L'IPSE a formulé des recommandations à l'effet que le CEN-ISSS doit : définir un ensemble de pratiques exemplaires volontaires et communes en Europe en matière de protection des données; établir un ensemble de clauses contractuelles génériques qui tiennent compte des exigences de l'article 17 de la Directive de l'UE; dresser un inventaire des pratiques de vérification de la protection des données; effectuer une enquête sur les programmes de sceaux comme base d'une meilleure normalisation; mettre au point une approche cohérente pour l'évaluation des incidences sur les avancées technologiques; et compiler et produire des documents de formation et de directives, sur des sujets ciblés, portant sur les enjeux relatifs à la normalisation en matière de protection de la vie privée.

Toutefois, l'IPSE n'a pas recommandé une norme de gestion qui s'appliquerait à l'Europe, prétendant qu'« il n'y avait pas de demande urgente de la part de l'industrie, en Europe, pour une norme de gestion en matière de protection de la vie privée » [traduction]. L'IPSE affirmait également que : « il était trop tôt pour entreprendre tout travail d'élaboration d'une norme européenne de gestion et que les intérêts de nature privée, en Europe, peuvent prendre une autre voie pour atteindre les objectifs, soit l'ISO, à partir des motions du COPOLCO, si désiré »[33] [traduction]. Les travaux du CEN ont pris la forme d'une série d'ateliers donnés par le Système de normalisation de la société de l'information (ISSS), notamment l'atelier portant sur la protection des données et de la vie privée – CEN/ISSS/WS/DPP. Cet atelier visait à « aider les organisations à se

management standard is desirable but is unlikely to materialize in the near future (for the reasons outlined), there are still ways in which existing management standards can be used to promote good data protection or privacy management internationally.

1) Organizations anywhere in the world that are otherwise registered to ISO 9000 series standards may incorporate privacy management into existing registration. Data protection authorities need to be aware of existing, and contemplated, registrations in order to encourage organizations to included personal information management as part of their "quality management systems".
2) Any organization that wishes a separate registration for privacy can always take the existing CSA Model Code, adapt it to its legal environment and organizational conditions and processes.
3) Any organization can "bridge" the existing CSA standard (Q830) to an existing or planned ISO 9000 registration.
4) Data protection agencies (as well as courts) can use their existing regulatory powers to encourage, or in some instances, require registration to a privacy standard when there are obvious privacy failures.

No privacy standard, and no standard registration, can substitute for properly enforced data protection legislation which applies to all organizations (public and private) within a given jurisdiction. Conversely, no law can be truly effective without appropriate mechanisms to allow organizations to truly say what they do, and do what they say.

Endnotes

[1] In this paper, we use the generic term "data protection authority" to refer to the family of independent bodies responsible for the oversight of national data protection or privacy statutes.

[2] See Colin J. Bennett and Charles D. Raab, The Governance of Privacy: Policy Instruments in Global Perspective (Cambridge: MIT Press, 2006).

[3] Quality assurance" refers to all the planned and systematic activities implemented within a quality system and demonstrated through internal and external quality audit.

[4] "Bridging" refers to the process whereby organizations declare their adherence to two

conformer à la directive sur la protection des données et à la législation nationale pertinente, en favorisant l'harmonisation des pratiques, une meilleure compréhension des pratiques détaillées ou des pratiques du secteur – tout en étant plus en mesure de les prévoir –, la participation au traitement des enjeux liés à la conformité technique des TIC et l'uniformité des évaluations et de la surveillance »[34] [traduction].

Les ateliers ont permis la production de plusieurs rapports en 2005 et en 2006, dont :

- un inventaire des pratiques de vérification de la protection des données;
- une analyse des technologies de protection de la vie privée, des technologies d'amélioration de la confidentialité (TAC), des systèmes de gestion de la protection de la vie privée et des systèmes de gestion de l'identité, les programmes de gestion à l'égard de ceux-ci et la nécessité de la normalisation;
- un contrat type pour favoriser le respect des obligations imposées par l'article 17 de la Directive de la protection des données 95/46/ EC (et guide de mise en œuvre);
- un cadre de vérification de la protection des renseignements personnels (Directive de l'UE EC 95/46) : *Part I: Baseline Framework – The protection of Personal Data in the EU*;
- un cadre de vérification de la protection des renseignements personnels (Directive de l'UE EC 95/46) : *Part II: Checklists, questionnaires and templates for users of the framework – The protection of Personal Data in the EU*[35].

En outre, les personnes qui ont participé à ces ateliers ont déterminé les secteurs et les éléments qui devaient faire l'objet d'autres travaux, en portant une attention particulière aux petites et aux moyennes entreprises, à l'auto-évaluation et à l'établissement de relations plus étroites entre les firmes et les organismes de réglementation.
Ces autres éléments sont :

- un ensemble de pratiques exemplaires dites volontaires, propres à l'Europe, pour la gestion de la protection de la vie privée, pour que les entreprises et les gestionnaires de données puissent être en mesure de se conformer à la Directive, dans la mesure du possible et si approprié, ainsi que pour respecter les différentes lois nationales de l'Europe et les autres exigences;
- des outils de vérification de la protection de la

complementary standards, and thereby save resources by engaging in only one conformity assessment process.

[5] Only this March, for example, the current chair of the U.S. Federal Trade Commission gave a speech about the importance of instilling a culture of privacy and security within the organization. Deborah Platt Majoras, "Building a Culture of Privacy and Security – Together," Speech to the IAPP Privacy Summit at: http:// www.ftc.gov/speeches/majoras/070307iapp.pdf

[6] James W. Kolka, ISO 9000: A Legal Perspective (Montclair: International Forum for Management Systems, 1998), p. 13.

[7] In this paper, the term "registration" is used for the process of independent verification and recognition on by a national or international official standards agency. "Certification" is used for other system of attestation that an organization complies with some other standards.

[8] http://www.simplyquality.org/howmany.htm

[9] Jaap van den Heuvel, Lida Koning, Ad J.J.C. Bogers, Marc Berg, Monique E.M. van Dijen, "An ISO 9001 quality management system in a hospital: Bureaucracy or just benefits?" International Journal of Health Care Quality Assurance 2005 Vol. 18, No. 5: 361 – 369

[10] International Trade Centre, Applying ISO 9000 Quality Management Systems (Geneva: 10 ITC, 1998), p.p. 13-14.

[11] ISO, as the publisher of standards, does not issue certificates of conformity to any standard. Certificates of conformity to specified standards are issued by certification/registration bodies which are independent of ISO and of the businesses they certify. There are over 740 certification or registration bodies worldwide. Source: International Accreditation Forum at: http://www.compad.com.au/clients/iaf/ indexPrev.php?updaterUrlPrev=articles&artId=24

[12] James W. Kolka, ISO 9000: A Legal Perspective (Montclair: International Forum for Management Systems, 1998), pp. 17%18.

[13] "The Michigan-based " Ponemon Institute© is dedicated to advancing responsible information on and privacy management practices in business and government. To achieve this objective, the Institute conducts independent research, educates leaders from the private and public sectors and verifies the privacy and data protection practices of organizations in a variety of industries." at http://www.ponemon.org/index.html. See http://www.ponemon.org/rim.html for more information regarding Responsible Information Management.

vie privée au sein de l'UE : en vue d'adopter une approche concrète qui s'appliquerait aux outils de vérification des gestionnaires de données, leur permettant d'effectuer des autoévaluations;
- un système interactif de technologie, afin de s'assurer que les nouveaux produits, les nouvelles technologies et les nouveaux services sont conformes aux lois pertinentes portant sur la protection des données et de la vie privée, puisque leur implantation dans tous les pays membres de l'UE pourrait représenter un défi pour l'industrie.

En outre, les organismes de réglementation estiment qu'ils ne sont pas toujours conscients de tout le potentiel qu'offrent les nouvelles technologies qui envahiront le marché dans un proche avenir.

International Security, Trust and Privacy Alliance (ISTPA)

International Security, Trust and Privacy Alliance (ISTPA) a été créée en 1999. Il s'agit d'une « alliance mondiale composée d'entreprises, d'institutions et de fournisseurs de technologies » [traduction]. Elle s'est donnée pour mission de « clarifier et de traiter les enjeux existants et à venir, liés à la sécurité, la confiance et la vie privée ». Aussi, elle porte « une attention particulière à la protection des renseignements personnels »[36] [traduction].

Elle a pour but :

- de mettre au point un cadre pour la protection des renseignements personnels et les données d'une organisation, qui définit les services en matière de sécurité, de protection de la vie privée et de confidentialité et leurs interrelations;
- de favoriser une meilleure compréhension de l'utilisation, de la gestion et des conséquences financières des technologies qui soutiennent la protection des données;
- d'effectuer des recherches, de réaliser des essais et des projets touchant l'interopérabilité pour aborder les enjeux importants liés à protection de la vie privée, la sécurité et la confidentialité;
- de fournir des conseils aux entreprises membres;
- d'offrir des forums internationaux pour discuter des enjeux et des solutions;

[14] The codification of the Fair Information Practices varies. They essentially boil down to the following. An organization (public or private):
- must be accountable for all the personal information in its possession
- should identify the purposes for which the information is processed at or before the time of collection
- should only collect personal information with the knowledge and consent of the individual (except under specified circumstances)
- should limit the collection of personal information to that which is necessary for pursuing the identified purposes
- should not use or disclose personal information for purposes other than those identified, except with the consent of the individual (the finality principle)
- should retain information only as long as necessary
- should ensure that personal information is kept accurate, complete and up-to-date should protect personal information with appropriate security safeguards
- should be open about its policies and practices and maintain no secret information system
- should allow data subjects access to their personal information, with an ability to amend it is inaccurate, incomplete or obsolete. From Bennett and Raab, p. 12.

[15] David H. Flaherty, Protecting Privacy in Surveillance Societies (Chapel Hill: University of North Carolina Press, 1989).

[16] Bennett and Raab, Ch. 6.

[17] For example, under the most popular progam (TRUSTe), there is no requirement for an on site examination of a website's privacy practices as a precondition for receiving the TRUSTe mark. Comprehensive examinations of an organization are only initiated "for cause" and when there is a privacy violation. Other programs, that of WebTrust, for instance, have more comprehensive auditing requirements. See: "Web Seals: A Review of Online Privacy Programs" A Joint Project of the Office of the Information and Privacy Commissioner/Ontario and the Office of the Federal Privacy Commissioner of Australia at: http://www.privacy.gov.au/publications/seals.html

[18] Increasingly, for example in the area of environmental sustainability, registration to one of the ISO 14000 standards is seen as a prerequisite for doing business with government in many areas. See, Michael McKloskey, ISO 14000: An Environmentalist's Perspective at:

- de défendre les intérêts de l'industrie et d'offrir à l'industrie des références sur les enjeux liés à la technologie en matière de protection de la vie privée;
- de faire connaître les travaux de l'ISTPA et sa mission.

Le cadre de protection de la vie privée 1.1 de l'ISTPA a été élaboré plus particulièrement à l'intention des agents et des personnes responsables de la protection de la vie privée au sein de leurs organisations respectives, mais également à l'intention des législateurs et des représentants du gouvernement qui souhaiteraient réglementer[37]. L'ISTPA a élaboré ce cadre qu'elle considère comme un « outil complet et précieux pour ceux qui mettent en œuvre des politiques de protection de la vie privée à l'aide de systèmes informatisés renfermant des renseignements permettant l'identification de la personne »[38] [traduction]. Le cadre élaboré avait également pour but d'aider les organisations à résoudre des problèmes techniques que pose la compréhension des normes de protection de la vie privée au sein de différentes juridictions. Ce cadre a par la suite été soumis à l'International System Security Engineering Association (ISSEA) comme une norme qui pourrait devenir une norme ISO de spécification accessible au public (PAS)[39], et il a également été remis aux commissaires à la protection des données et de la vie privée, lors d'une conférence internationale à Wroclaw (Pologne) en 2004.

Du point de vue historique, les autorités de protection des données n'ont pas participé intensément aux activités relatives à l'élaboration de normes. Cependant, le groupe de travail qui a étudié l'article 29 a émis son opinion le 29 mai 1997, pour réitérer son soutien envers de telles initiatives qui « favorisaient, de façon significative, la protection de droits fondamentaux et de la vie privée, à l'échelle planétaire »[40] [traduction]. À Wroclaw, les commissaires ont adopté une résolution qui stipule qu'« une norme mondiale en matière de protection de la vie privée, et plus particulièrement une norme visant la technologie de protection de la vie privée doit être élaborée par l'ISO, norme qui soutiendrait la mise en œuvre de règles juridiques sur la protection des données et de la vie privée dans les pays où elles ont été adoptées et la formulation de règles dans les pays qui n'en ont pas encore adopté» [traduction]. Les commissaires ont également exprimé leurs préoccupations : les initiatives de l'ISTPA et du

http://www.ecologia.org/ems/iso14000/resources/opinions/mccloskey96.html

[19] There have been examples of court-ordered registration to ISO 14000 as penalties for environmental pollution.

[20] The ISO/IEC Guides and the IAF Guidance to them are designed to ensure that certification/registration bodies are both competent to carry out the work involved and are operated independently of businesses that are certified. Source, International Accreditation Forum (IAF), Inc. website at: http:// www.compad.com.au/clients/iaf/indexPrev.php?updaterUrlPrev=articles&artId=24

[21] The American National Standards Institute (ANSI) for example has issued standards on privacy impact assessments, the privacy of communication in electronic funds transfers, standards for electronic health records, telecommunications security in ISDN and so on. See: http://webstore.ansi.org/ansidocstore/find.asp?

[22] CSA, PLUS 8830 – Implementing Privacy Codes of Practice, Colin J. Bennett, 22 August 1995.

[23] Organisation for Economic Co-operation and Development (OECD) (1981), Guidelines on the Protection of Privacy and Transborder Flows of Personal Data, (Paris: OECD).

[24] http://www.privcom.gc.ca/information/ar/200607/2006_pipeda_e.asp#028

[25] See e.g., John Lawford, Consumer Privacy under PIPEDA: How are we Doing? (Public Interest Advocacy Centre: November 2004); Rajen Akalu et al. Implementing PIPEDA: A Review of Internet Privacy Statements and Online Practices (May 2005) at http://pipedaproject.atrc.utoronto.ca/index.php?option=com_content&task=view&id=66&Itemid=80

[26] See the arguments in: Colin J. Bennett, Prospects for an International Standard for the Protection on of Personal Information: A Report to the Standards Council of Canada (August 1997) at: http://web.uvic.ca/~polisci/bennett/research/iso.htm

[27] www.27000.org Commission (IEC).

[28] 2006 privacy-related publications include: Information technology - Security techniques Selection, deployment and operations of intrusion detection systems and Multimedia security - Guideline for privacy protection of equipment and systems in and out of use, with work in progress on Multimedia Security - Guideline for privacy protection of equipment and systems in use and disused % Part 2: Software method for privacy protection (TC 100). See http://www.iec.ch/cgi%bin/procgi.pl/www/iecwww.p?wwwlang=E&wwwprog=seabox1.p&seabox1=privacy.

JTC 1 favorisent l'élaboration de cadres de gestion de la protection de la vie privée qui tiennent compte de l'historique de la loi visant la protection des données en Europe. Ils rappellent d'ailleurs que « l'élaboration d'une norme internationale de protection de la vie privée doit reposer sur des pratiques équitables de traitement de l'information, ainsi que sur les notions de rareté des données, de minimisation et d'anonymat »[41]. L'ISTPA est en voie de produire une nouvelle version de son cadre de protection de la vie privée pour tenir compte des préoccupations soulevées lors de la conférence internationale, dans l'espoir de soumettre de nouveau le document aux fins d'examen du cadre qui pourrait devenir une norme ISO.

V. Conclusion : participation des autorités de protection des données

À la fin de l'année 2007, voici le portrait de la normalisation en matière de protection de la vie privée :

- une norme nationale de protection de la vie privée pour le Canada, qui est presque superflue, en raison de l'existence de la *LPRPDÉ*;
- d'importantes avancées pour le JTC 1 de l'ISO, en vue d'entamer les discussions concernant les normes techniques de base, dont certaines proposent des éléments clés et supposent des conséquences;
- un travail considérable a été accompli en collaboration avec le CEN-ISSS sur la vérification de la protection des données et les processus de passation des contrats, ainsi que sur les technologies d'amélioration de la protection de la vie privée. Cependant, nous ne savons pas encore la façon dont le fruit de ce travail pourra être intégré dans le cadre des tâches quotidiennes des autorités de protection des données, et nous savons encore moins comment les entreprises européennes assureront la conformité en matière de protection de la vie privée.

L'idée d'une norme de gestion d'ordre général – une version internationale du code type de la CSA – a été difficile à concrétiser. Certaines raisons peuvent expliquer cet état de fait :

- une certaine réticence de la part des organismes rédacteurs de normes à

29 http://www.ni.din.de/sc27

30 http://www.itu.int/ITU%T/studygroups/com17/ict/docs/ISOandIEC.pdf

31 From the CEN website, 31 , at: http://www.cen.eu/cenorm/aboutus/index.asp Its complex hierarchy and relationships are well% depicted graphically at http://www.cen.eu/cenorm/aboutus/structure+/thecensystem/structure1.ppt.

32 Initiative for Privacy Standardization in Europe: Final Report at: http://ec.europa.eu/enterprise/ict/policy/standards/ipse_finalreport.pdf

33 Ibid, p. 51.

34 CEN website, at: http://www.cen.eu/cenorm/businessdomains/businessdomains/isss/activity/wsdpp.asp

35 CEN website, at: http://www.cen.eu/cenorm/businessdomains/businessdomains/isss/activity/wsdpp.asp
The CWAs are available for download at: http://www.cen.eu/cenorm/businessdomains/businessdomains/isss/cwa/dppcwa.asp

36 From http://www.istpa.org/about/index.htm Members and affiliates include AMD, BITS, The Technology Group for the Financial Services Roundtable, Carnegie Mellon University, Computer Associates International, CYVA Research Corporation, DiscoverTek, EWA Information and Infrastructure Technologies, Inc., Gemplus, Government of Alberta, Office of the CIO, GSR Strategic Consulting, Harry Lewis, Esq., HiSoftware Company, IBM, International Systems Security Engineering Association, Jonathan Moore, Johns Hopkins University, Kendall Scott, KLS Consulting, LLP, Motorola, NCR, OneName Corporation, Potter Group, Seagate Technology, TVC UK Ltd, TRUSTe, Vanguard Integrity Professionals, Wave Systems Corporation

37 http://www.istpa.org/faqs/framework.htm

38 Borking, John J., Privacy Standards for Trust, October, 2005, p. 5 at: http://www.privacyconference2005.org/fileadmin/PDF/borking.pdf

39 A PAS is a "A normative document representing the consensus within a working group", so less than a full% fledged standard: http://www.iso.org/iso/en/stdsdevelopment/whowhenhow/proc/deliverables/iso_pas.html

40 http://ec.europa.eu/justice_home/fsj/privacy/workinggroup/wpdocs/1997_en.htm

41 Resolution on a Draft ISO Privacy Framework Standard, ISO/IEC JTC1 SC36# N1231, 2006% 02%15, available at

s'immiscer dans une « zone » faisant habituellement partie des droits de la personne;
- le scepticisme de la part des défenseurs de la vie privée et des organismes de réglementation quant à la pertinence de faire appel à un autre groupe d'institutions internationales pour traiter des enjeux;
- les avocats et les organismes de réglementation craignent qu'une norme de gestion d'ordre général ne sape les lois existantes en matière de protection de la vie privée;
- face à certains éléments, les intérêts du secteur privé font en sorte que ce dernier s'oppose farouchement à l'idée d'une norme de gestion d'ordre général;
- la multiplication des sceaux et des certifications dans Internet, qui octroie aux entreprises un semblant de conformité en matière de protection de la vie privée, sans que ces dernières soient obligées de se soumettre à un processus d'enregistrement rigoureux en vue de se conformer à une norme.

Certains se demandent alors s'il est encore temps d'instaurer une norme de gestion en matière de protection de la vie privée. Néanmoins, étant donné les circonstances actuelles où les effractions à la protection des données sont fréquentes, l'idée d'un système de normes pour la protection de la vie privée, qui pourrait soutenir les lois existantes, n'a jamais été aussi pertinente.

Le processus d'obtention et la conservation d'une certification à une norme de protection de la vie privée peut alléger le fardeau des agences de protection de la vie privée qui constituent les seules autorités de surveillance et de contrôle. Dans un contexte de traitement mondial des renseignements personnels, l'examen approfondi des lois et des contrats ne garantit pas aux autorités de protection des données que celles-ci soient respectées de la part de la juridiction destinataire. Le fait de vouloir se conformer à une norme, ce qui suppose des vérifications indépendantes et régulières, pourrait renforcer la certitude que les pratiques en matière de protection des données des organisations destinataires sont adéquates, peu importe où se trouvent ces organisations et peu importe leur secteur d'activités. La certification peut également fournir de meilleures garanties aux consommateurs désireux de faire affaire avec des

http://jtc1sc36.org/doc/N1201%N1250.html
The subsequent organization (the Wroclaw Foundation), which was formed to address procedural issues and facilitate their formal recognition in the standard's development, did not realize its goal.

* * *

organisations qui mettent l'accent sur la protection de la vie privée. Les garanties sont « meilleures » parce qu'une organisation qui entérine de bonnes pratiques en matière de protection de la vie privée a fait l'objet de vérifications par un organisme indépendant, et aussi parce que, émanant des autorités responsables des normes, les exigences sont strictes, rigoureuses et cohérentes.

Comme il est souhaitable de mettre en application une norme internationale de gestion de la protection de la vie privée mais qu'il n'est pas possible de concrétiser ce projet à court terme (pour les raisons susmentionnées), il est possible de prendre des moyens grâce auxquels les normes de gestion existantes peuvent servir à assurer une bonne protection des données ou une bonne gestion de la protection de la vie privée, et ce, à l'échelle internationale.

1) Peu importe où elles se trouvent, les organisations qui se sont enregistrées en vue de se conformer à la série de normes ISO 9000 pourraient intégrer les pratiques de gestion de la protection de la vie privée dans la certification. Les autorités de protection des données doivent connaître les certifications existantes afin d'encourager les organisations à intégrer la gestion de la protection des renseignements personnels dans leur « système de gestion de la qualité ».
2) Toute organisation qui souhaite une certification distincte en matière de protection de la vie privée a toujours la possibilité de se saisir du Code type de la CSA, de le modifier en fonction des dispositions légales qui la concerne ainsi qu'en fonction des conditions et des processus organisationnels.
3) Toute organisation peut établir un lien avec une norme existante de la CSA (Q830) ou avec une norme ISO 9000 à laquelle elle désire se conformer.
4) Les agences de protection des données (de même que les tribunaux) peuvent exercer leur pouvoir de réglementation afin d'encourager – ou, dans certains cas, exiger – l'enregistrement en vue de se conformer à une norme de protection de la vie privée lorsque des failles évidentes ont été constatées dans la protection de la vie privée.
5) Aucune norme de protection de la vie privée et aucun processus d'enregistrement en vue de se conformer à une norme ne peut remplacer une réglementation de la protection des données qui s'applique à toutes les

organisations (des secteurs public et privé) à l'intérieur d'une juridiction donnée. À l'inverse, une loi ne peut être réellement efficace qu'en présence de mécanismes appropriés qui permettent aux organisations de dire vraiment ce qu'elles font et de faire ce qu'elles disent.

Notes en bas de page

[1] Dans ce document, nous utilisons le terme générique « autorité de protection des données » pour faire référence aux organismes indépendants responsables de la surveillance de la protection des données ou de la législation relative à la vie privée.

[2] Voir Colin J. Bennett et Charles D. Raab, The Governance 2 of Privacy : Policy Instruments in Global Perspective (Cambridge, MIT Press, 2006).

[3] L'« assurance de la qualité » fait référence à toutes les activités planifiées et systématiques mises en œuvre dans le cadre d'un système de contrôle de la qualité et qui ont fait leurs preuves, grâce à une vérification interne et externe.

[4] « Faire le pont » fait référence au processus par lequel les organisations déclarent vouloir respecter les deux normes complémentaires, et, ainsi, réaliser des économies en matière de ressources, en participant à un seul processus de vérification de la conformité.

[5] Uniquement au mois de mars, par exemple, le président actuel de la U.S. Federal Trade Commission a prononcé un discours sur l'importance de l'implantation d'une culture de la vie privée et de la sécurité au sein de l'organisation. Deborah Platt Majoras, « Building a Culture of Privacy and Security – Together » : exposé donné lors d'un sommet sur la vie privée, organisé par l'International association of privacy professionals (IAPP), qui peut être consulté à l'adresse : http://www.ftc.gov/speeches/majoras/070307iapp.pdf.

[6] James W. Kolka, ISO 9000: A Legal Perspective (Montclair, International Forum for Management Systems, 1998, p. 13).

[7] Dans cet article, le terme « enregistrement » sert à désigner le processus de vérification et de reconnaissance réalisé par un organisme – national ou international – de normes officielles. Le terme « certification » est utilisé pour d'autres mécanismes d'attestation auxquels une organisation se conforme en respectant d'autres

normes.

[8] http://www.simplyquality.org/howmany.htm.

[9] Jaap van den Heuvel, Lida Koning, Ad J.J.C. Bogers, Marc Berg, Monique E.M. van Dijen, « An ISO 9001 quality management system in a hospital : Bureaucracy or just benefits? », International Journal of Health Care Quality Assurance, 18(5) (2005) p. 361-369.

[10] International Trade Centre, Applying ISO 9000 Quality Management 10 Systems (Genève, ITC, 1998, p. 13‑14).

[11] ISO, à titre d'éditeur des normes, n'octroie pas de certificats de conformité à toute norme. Les certificats de conformité à des normes particulières sont émis par des organismes de certification ou d'enregistrement, qui sont indépendants de l'ISO et des entreprises qu'ils certifient. Il existe plus de 740 organismes de certification ou d'enregistrement partout dans le monde. Source : International Accreditation Forum à l'adresse : http://www.compad.com.au/clients/iaf/indexPrev.php?updaterUrlPrev=articles&artId=24 (site australien unilingue anglais)

[12] James W. Kolka, ISO 9000 : A Legal Perspective (Montclair, International Forum for Management Systems, 1998, p. 17‑18).

[13] Le Ponemon Institute©, dont l'une de ses succursales se trouve dans le Michigan, « cherche à améliorer les pratiques de gestion responsable des renseignements et de la vie privée, au sein des entreprises et du gouvernement. Pour atteindre cet objectif, l'institut mène des recherches indépendantes, forment des dirigeants des secteurs privé et public et vérifie les pratiques en matière de protection des données et de la vie privée des organisations relevant de différentes industries » [traduction] à l'adresse : http://www.ponemon.org/index.html (site Internet en anglais). Consulter le site à l'adresse : http://www.ponemon.org/rim.html pour en savoir plus au sujet de la gestion responsable des renseignements.

[14] La codification des pratiques équitables de traitement de l'information varie. Les pratiques se résument essentiellement aux points ci-dessous. Une organisation (du secteur public ou privé) :

- doit être responsable de tous les renseignements personnels dont elle a la gestion;
- doit déterminer les fins auxquelles des renseignements personnels sont recueillis doivent être déterminées par l'organisation avant la collecte ou au moment de celle-ci;

- doit recueillir uniquement les renseignements personnels avec le consentement éclairé de la personne concernée (sauf en certaines circonstances particulières explicitées);
- doit se limiter à recueillir les renseignements personnels qui sont nécessaires aux fins déterminées;
- ne peut utiliser ou communiquer des renseignements personnels qu'à des fins déterminées, sauf si la personne concernée y consent (principe de la finalité);
- doit conserver les données uniquement pour une période jugée nécessaire;
- doit s'assurer que les renseignements personnels sont conservés de façon adéquate et que l'information est complète et à jour;
- doit protéger les renseignements personnels à l'aide de mesures de sécurité adéquats;
- doit faire preuve de transparence relativement à ses politiques et à ses pratiques et ne soutenir aucun système de renseignements secrets;
- doit permettre l'accès aux données des renseignements personnels détenus et à des fonctions pour modifier les données inexactes, incomplètes ou désuètes. (Inspiré de Bennett et Raab, p. 12.)

[15] David H. Flaherty, Protecting Privacy in Surveillance Societies (Chapel Hill, University of North Carolina Press, 1989).

[16] Bennett et Raab (chapitre 6).

[17] Par exemple, dans le cadre du plus populaire programme (TRUSTe), il n'y avait aucune exigence relativement à l'examen sur place des pratiques en matière de protection de la vie privée relativement à l'utilisation d'un site Internet, à titre de condition préalable pour l'octroi du sceau TRUSTe. Les examens exhaustifs d'une organisation sont effectués uniquement « pour un motif valable » et en cas de non respect de la vie privée. D'autres programmes comme WebTrust par exemple, possèdent des exigences de vérification plus complètes. Consulter : « Web Seals: A Review of Online Privacy Programs », un projet conjoint du Commissaire à l'information et à la protection de la vie privée/Ontario (CIPVP) et du Commissariat fédéral à la protection de la vie privée de l'Australie à l'adresse : http:// www.privacy.gov.au/publications/seals.html.

[18] L'enregistrement à l'une des normes, comme par exemple ISO 1400, dans le domaine de la durabilité écologique, est de plus en plus considérée comme un préalable pour faire affaire avec le gouvernement, et ce, dans plusieurs domaines. Voir l'article de Michael McKloskey

intitulé « ISO 14000 : An Environmentalist's Perspective » à l'adresse : http://www.ecologia.org/ems/iso14000/resources/opinions/mccloskey96.html.

[19] Il existe des exemples de cas de certifications ISO 14000, ordonnées par la cour, à titre de sanction pour avoir pollué l'environnement.

[20] Les guides ISO et de la CEI – ainsi que les directives de l'International Accreditation Forum (IAF) pour ces guides – sont conçus pour s'assurer que les organismes de certification ou d'enregistrement sont tous deux compétents pour réaliser le travail et qu'ils fonctionnent de façon indépendante des entreprises qui sont certifiées. Source : site Internet de l'International Accreditation Forum (IAF) Inc. à l'adresse suivante : http://www.compad.com.au/clients/iaf/indexPrev.php?updaterUrlPrev=articles&artId=24.

[21] L'American National Standards Institute (ANSI), par exemple, a établi des normes relativement à l'évaluation des facteurs relatifs à la vie privée (ÉFVP), la protection de la vie privée lors du transfert de fonds par voie électronique, les dossiers électroniques de santé, la sécurité des télécommunications dans un réseau numérique avec intégration des services (RNIS), etc. Consulter : http://webstore.ansi.org/ansidocstore/find.asp?

[22] Colin J. Bennett, CSA, PLUS 8830 – Implementing Privacy Codes of Practice, août 1995.

[23] Organisation de coopération et de développement économiques (OCDE) (1981), Lignes directrices régissant la protection de la vie privée et le flux transfrontalier de données à caractère personnel. (Paris, OCDE).

[24] http://www.privcom.gc.ca/information/ar/200607/2006_pipeda_f.asp#028.

[25] Voir p. ex. John Lawford, Consumer Privacy under PIPEDA : How are we Doing? (Public Interest Advocacy Centre, novembre 2004); Rajen Akalu et al. « Implementing PIPEDA : A Review of Internet Privacy Statements and Online Practices » (mai 2005), article disponible à l'adresse : http://pipedaproject.atrc.utoronto.ca/index.php?option=com_content&task=view&id=66&Itemid=80 (site unilingue anglais).

[26] Lire les arguments dans : Colin J. Bennett, Prospects for an International Standard for the Protection of Personal Information : A Report to the Standards Council of Canada (août 1997) disponible sur le site Internet à l'adresse : http://web.uvic.ca/~polisci/bennett/research/iso.htm (site unilingue anglais).

[27] www.27000.org – Commission (CEI).

[28] Voici quelques publications de l'année 2006 portant sur la protection de la vie privée : Information technology - Security techniques - Selection, deployment and operations of intrusion detection systems; Selection, deployment and operations of intrusion detection systems and Multimedia security - Guideline for privacy protection of equipment and systems in and out of use, with work in progress on Multimedia Security; Guideline for privacy protection of equipment and systems in use and disused - Part 2: Software method for privacy protection (TC 100). Consulter le site Internet à l'adresse : http://www.iec.ch/cgi-bin/procgi.pl/www/iecwww.p?wwwlang=e&wwwprog=seabox1.p&progdb=db1&seabox1=privacy.

[29] http://www.ni.din.de/sc27 (site Internet en anglais).

[30] http://www.itu.int/ITU%T/studygroups/com17/ict/docs/ISOandIEC.pdf.

[31] Sur le site Internet du CEN à l'adresse : http://www.cen.eu/cenorm/aboutus/index.asp (site en anglais). La hiérarchie et les relations complexes sont bien illustrées dans l'image disponible à l'adresse : http://www.cen.eu/cenorm/aboutus/structure+/structure1.pdf

[32] Initiative de normalisation de la protection de la vie privée en Europe : il est possible de consulter le rapport final http://ec.europa.eu/enterprise/ict/policy/standards/ipse_finalreport.pdf

[33] Ibid., p. 51.

[34] Site Internet du CEN : http://www.cen.eu/cenorm/businessdomains/businessdomains/isss/activity/wsdpp.asp.

[35] Site Internet du CEN : http://www.cen.eu/cenorm/businessdomains/businessdomains/isss/activity/wsdpp.asp. Il est possible de télécharger les normes ISO/CEI à partir du site Internet à l'adresse : http://www.cen.eu/cenorm/businessdomains/businessdomains/isss/cwa/dppcwa.asp.

[36] Extrait de : http://www.istpa.org/about/index.htm. Voici quelques-uns des membres et des 36 sociétés affiliées : AMD, BITS, groupe de technologie de la Financial Services Roundtable, Carnegie-Mellon Institute, Computer Associates International, CYVA Research Corporation, DiscoverTek, EWA Information and Infrastructure Technologies Inc., Gemplus, gouvernement de l'Alberta, CIO, GSR Strategic Consulting, Harry Lewis, Esq., HiSoftware Company, IBM, International Systems Security Engineering

Association, Jonathan Moore, Johns Hopkins University, Kendall Scott, KLS Consulting, LLP, Motorola, NCR, OneName Corporation, Potter Group, Seagate Technology, TVC UK Ltd, TRUSTe, Vanguard Integrity Professionals, Wave Systems Corporation.

[37] http://www.istpa.org/faqs/framework.htm (site unilingue anglais).

[38] Article de John J Borking intitulé « Privacy Standards for Trust » (octobre 2005, p. 5) que l'on peut consulter : http://www.privacyconference2005.org/fileadmin/PDF/borking.pdf (disponible uniquement en anglais).

[39] La spécification accessible au public (ou PAS) est « Un document normatif issu d'un consensus d'un groupe de travail », ce qui n'équivaut pas à une norme en bonne et due forme : http://www.iso.org/iso/en/stdsdevelopment/whowhenhow/proc/deliverables/iso_pas.html.

[40] http://ec.europa.eu/justice_home/fsj/privacy/workinggroup/wpdocs/1997_fr.htm.

[41] La résolution portant sur l'ébauche d'une norme du cadre de gestion de la protection de la vie privée, par l'ISO, soit ISO/CEI JTC 1 SC n° 36 N1231 (15 février 2006), est disponible à l'adresse : http://jtc1sc36.org/doc/N1201%N1250.html. L'organisation (la Wroclaw Foundation) qui a par la suite été créée afin d'examiner les enjeux liés aux procédures et favoriser la reconnaissance officielle de l'élaboration de normes, n'a pas atteint ses buts.

29E CONFÉRENCE INTERNATIONALE DES COMMISSAIRES
À LA PROTECTION DES DONNÉES ET DE LA VIE PRIVÉE

LES HORIZONS DE LA PROTECTION DE LA VIE PRIVÉE

TERRA INCOGNITA

PRIVACY HORIZONS

29TH INTERNATIONAL CONFERENCE OF
DATA PROTECTION AND PRIVACY COMMISSIONERS

Faire avancer la protection de la vie privée au Canada : Développer une stratégie canadienne de normalisation

Atelier tenu à Ottawa le 22 février 2007

Advancing the Privacy Agenda in Canada: Developing a Canadian Standardization Strategy

Workshop held February 22, 2007 – Ottawa

Office of the Privacy Commissioner of Canada
Commissariat à la protection de la vie privée du Canada

Résumé

Le 22 février 2007, le Commissariat à la protection de la vie privée du Canada et des partenaires du Système national de normes, comprenant notamment l'Association canadienne de normalisation, l'Office des normes générales du Canada et le Conseil canadien des normes, ont parrainé un atelier sur la protection de la vie privée et la normalisation au Canada. Cet atelier, auquel ont participé 62 intervenants représentant des entreprises, des praticiens du domaine de la protection des renseignements personnels, le gouvernement, des organismes de défense des consommateurs, des organismes publics, des universités et des organismes d'élaboration de normes, constituait la première étape de la création d'une stratégie canadienne de normalisation et d'une feuille de route en vue de l'avancement de la protection de la vie privée au Canada.

Dans le cadre de l'atelier, les leçons apprises ont fait l'objet de discussions et les facteurs indispensables au succès de l'élaboration et de la mise en œuvre d'une stratégie nationale de normalisation ont été déterminés. Les principaux facteurs de réussite du projet comprenaient la nécessité de bien analyser la rentabilité du projet, d'obtenir l'engagement des intervenants, de fixer des objectifs à long terme, de produire des outils pratiques et des solutions applicables à des échelles variables, de se fixer des buts réalistes, de faire preuve de transparence et de se doter des ressources nécessaires.

On a proposé les thèmes suivants pour l'atelier :

- *La normalisation comble les lacunes* ─ Faire des renvois, dans la législation, à des normes facultatives et positionner la normalisation en complément à la législation.

- *Les normes de référence sont utiles* ─ Des exigences de base accompagnées d'un ensemble commun de « principes », avec l'application des normes additionnelles propres à chacun des secteurs.

- *Concentration sur les besoins spéciaux* ─ Combler les besoins spéciaux au moyen d'exigences supplémentaires (p. ex. les chercheurs en santé, l'impartition, les échanges transfrontaliers d'information, les PME).

Executive Summary

On February 22, 2007, the Office of the Privacy Commissioner of Canada and partners in the National Standards System, including: the Canadian Standards Association, the Canadian General Standards Board, and the Standards Council of Canada, sponsored a workshop on the topic of privacy and standardization in Canada. Attended by 62 invited stakeholders representing business, privacy practitioners, government, consumer and public organizations, academia and standards development, the workshop was the first step in the establishment of a Canadian standardization strategy and roadmap for advancing privacy in Canada.

During the workshop lessons learned were discussed and key success factors to the development and implementation of a national standardization strategy were captured. Key success factors included the need for a clear business case, stakeholder engagement, long-term objectives, practical tools, scalable solutions, realistic goals, transparency, and resources.

The following key workshop themes were identified:

- *Standardization bridges gaps* – Referencing of voluntary standards in legislation and position standardization as complimentary to legislation.

- *Baseline standards are useful* – Baseline requirements with a common set of "principles" with additional sector-specific applications of standards.

- *Focus on special needs* – Address special needs with supplementary requirements (e.g., health researchers, outsourcing, trans-boarder sharing of information, SMEs)

- *Demonstrating conformance* – Importance of ability to demonstrate conformance through self-assessment or third party in order to measure effectiveness.

- *Sharing best practices* – An inclusive process is needed including all stakeholder groups.

- *Timing is critical* – Must start now to see benefits in the future.

- *Preuve de conformité* — Importance de pouvoir prouver la conformité par l'autoévaluation ou l'évaluation par un tiers, afin d'évaluer l'efficacité des mesures.

- *Mise en commun des pratiques exemplaires* — Il faut un processus d'inclusion, réunissant tous les groupes d'intervenants.

- *Le temps presse* — Il faut commencer maintenant pour pouvoir profiter des avantages dans l'avenir.

- *Obtenir la participation des intervenants* — Commencer avec une approche claire et transparente pour obtenir l'engagement des intervenants et bien analyser la rentabilité du projet pour le milieu des affaires.

Contexte

Le 22 février 2007, le Commissariat à la protection de la vie privée du Canada et des partenaires du Système national de normes, comprenant notamment l'Association canadienne de normalisation, l'Office des normes générales du Canada et le Conseil canadien des normes, ont parrainé un atelier sur la protection de la vie privée et la normalisation au Canada. Cet atelier, auquel ont participé 62 intervenants représentant des entreprises, des praticiens du domaine de la protection des renseignements personnels, le gouvernement, des organismes de défense des consommateurs, des organismes publics, des universités et des organismes d'élaboration de normes, constituait la première étape de la création d'une stratégie canadienne de normalisation et d'une feuille de route en vue de l'avancement la protection de la vie privée au Canada.

Les objectifs de l'atelier étaient les suivants :

- *Permettre aux participants de mieux comprendre le paysage actuel de la protection de la vie privée au Canada;*
- *Explorer les problèmes actuels liés à la protection de la vie privée auxquels la normalisation pourrait fournir des outils et des solutions, pour le Canada et l'étranger;*
- *Mettre en place un forum réunissant les experts canadiens du domaine afin d'envisager des façons de faire avancer la normalisation en matière de protection de la*

- *Engaging stakeholders* – Start with clear and transparent approach to gain commitment and build a business case for the business community.

Background

On February 22, 2007, the Office of the Privacy Commissioner of Canada and partners in the National Standards System, including: the Canadian Standards Association, the Canadian General Standards Board, and the Standards Council of Canada, sponsored a workshop on the topic of privacy and standardization in Canada. Attended by 62 invited stakeholders representing business, privacy practitioners, government, consumer and public organizations, academia and standards development, the workshop was the first step in the establishment of a Canadian standardization strategy and roadmap for advancing privacy in Canada.

The Workshop objectives were to:

- *Enhance participants understanding of the current landscape of privacy protection in Canada;*
- *Explore current privacy issues where standardization could provide tools and solutions for Canada and beyond;*
- *Provide a forum to bring together Canadian expert stakeholders to explore and build consensus on a 'Way Forward' for privacy standardization in Canada, and*
- *Explore technical and non-technical standardization solutions for Privacy.*

Format of Workshop

The workshop was designed to stimulate dialogue and to obtain feedback from participants to help create a roadmap covering the current landscape for privacy standardization activities, needs, issues and potential opportunities. The format included presentations from keynote speakers followed by breakout sessions on 4 streams in the morning and 4 different streams in the afternoon. This report highlights the key themes identified by keynote speakers as well as a summary of the outcomes from the 8 breakout sessions.

vie privée au Canada et d'établir un consensus à ce sujet;
- *Explorer des solutions techniques et non techniques à la normalisation de la protection de la vie privée.*

Formule de l'atelier

L'atelier a été conçu de façon à encourager le dialogue et à obtenir les opinions des participants afin qu'ils participent à la création d'une feuille de route couvrant l'éventail actuel des activités, des besoins, des problèmes et des possibilités en ce qui a trait à la normalisation de la protection de la vie privée. La formule comprenait des présentations par des conférenciers principaux, suivies de séances en groupes portant sur quatre thèmes l'avant-midi et quatre thèmes différents l'après-midi. Le présent rapport souligne les principaux thèmes dégagés par les conférenciers et résume les résultats des huit séances de groupes.

Le rôle des normes de protection de la vie privée au Canada

- Traiter de questions d'harmonisation dont la législation ne traite pas;
- Traiter de pratiques particulières;
- Traiter des préoccupations liées aux nouvelles; technologies (p. ex. l'identification par radiofréquence, la biométrie, l'information génétique, la localisation, l'exploration et le profilage de données, la vidéosurveillance, etc.);
- Traiter de questions de base telles que la limitation de la collecte d'information, la conservation de données, les mesures de sécurité, etc.;
- Traiter des nouvelles questions publiques et stratégiques, comme la circulation transfrontalière des données et le vol d'identité;
- Contribuer aux évaluations des facteurs relatifs à la vie privée, aux évaluations des menaces et des risques et aux vérifications.

Leçons apprises liées aux principaux facteurs de succès

- Nécessité de présenter un dossier clair pour la normalisation

The Role for Privacy Standards in Canada

- To address harmonization issues not captured in legislation;
- To address specific practices;
- To address new technology concerns (e.g. RFIDs, biometrics, genetic information, location tracking, data mining and profiling, video surveillance, etc.);
- To address baseline issues such as limiting collection, data retention, safeguards, etc.;
- To address emerging public and policy issues such as transborder flows and identity theft; and
- For Privacy Impact Assessments, Threat/Risk Assessments and Audits.

Lessons Learned related to Key Success Factors

- Need to present a clear business case for standardization
- Focus on long term objectives
- Make standards offerings relevant and realistic by providing practical tools and realistic goals
- Provide an Inclusive process with the engagement of all stakeholders
- Ensure transparency of the standardization process
- Need for resources to support exercise
- Solutions must be scaleable – needs of small and medium-sized organizations must be considered in the development of solutions
- Focus on standards products that bridge current gaps in the privacy landscape
- Stakeholders need to agree on the agenda and the process

Questions to be Addressed in Developing a Standardization Strategy

- Do we need new standards in Canada?
- Should we be looking at global standards?
- Who takes the lead role?
- How do they integrate with legislation?
- How do organizations adopt them and certify to them?
- What is the value add for organizations?
- What is the value add for the public?

- Concentration sur les objectifs à long terme
- Rendre l'offre des normes pertinente et réaliste en présentant des outils pratiques et des objectifs réalistes
- Mettre en place un processus d'inclusion et obtenir la participation de tous les intervenants
- Assurer la transparence du processus de normalisation
- Nécessité de se doter de ressources pour soutenir ces activités
- Les solutions doivent pouvoir s'appliquer à des échelles variables — il faut tenir compte des besoins des petites et moyennes organisations dans l'élaboration des solutions
- Se concentrer sur des produits normatifs qui comblent les lacunes actuelles dans le domaine de la protection de la vie privée
- Les intervenants doivent s'entendre sur le programme et le processus

Questions à traiter dans le cadre de l'élaboration d'une stratégie de normalisation

- Avons-nous besoin de nouvelles normes au Canada?
- Devrions-nous envisager des normes mondiales?
- Qui prend la direction des travaux?
- Comment ces normes s'intègrent-elles à la législation?
- Comment les organisations les adoptent-elles et les attestent-elles?
- Quelle est la valeur ajoutée pour les organisations?
- Quelle est la valeur ajoutée pour le public?

Principaux thèmes de l'atelier

La normalisation comble les lacunes
- Elle aide à la mise en œuvre de la législation et au respect des exigences relatives à la vie privée
- Elle permet d'inclure dans la législation des renvois à des normes facultatives
- La normalisation complète et enrichit la législation

Normes de référence
- Exigences de base à l'échelle nationale

Key Workshop Themes

Standardization Bridges Gaps
- Assist with implementation of privacy legislation and requirements
- Referencing of voluntary standards in legislation
- Standardization is complimentary and supplementary to legislation

Baseline Standards
- Baseline requirements at National level
- Common set of "principles" (National and International)
- Sector-specific applications of standards

Focus on Special Needs
- Special needs addressed by supplementary requirements (e.g., health researchers)
- Outsourcing
- Trans-boarder sharing of information (global issue)
- Small and medium sized organizations (scalability)
- Others to be identified

Demonstrating Conformance
- Audit tools (ability to demonstrate conformance through self-assessment or third party)
- Measure effectiveness
- Management System Standards

Sharing Best Practices
- Need for inclusive process, including all stakeholder groups
- Need for information sharing resource

Timing is Critical
- Must start now to see benefits in the future

Engaging Stakeholders
- Start with clear and transparent approach to gain commitment
- Business case for the business community
- Funding

Breakout Session 1: Standardization Needs

STREAM 1: Legal and Regulatory

The objective of this session was to identify the

- Ensemble commun de « principes » (nationaux et internationaux)
- Application des normes propres à chacun des secteurs

Concentration sur les besoins spéciaux
- Combler les besoins spéciaux au moyen d'exigences supplémentaires (p. ex. les chercheurs en santé)
- L'impartition
- Les échanges transfrontaliers d'information (problème mondial)
- Les petites et moyennes organisations (échelles variables)
- Autres besoins spéciaux à déterminer

Démontrer la conformité
- Outils de vérification (capacité de prouver la conformité par une autoévaluation ou l'évaluation par un tiers)
- Mesure de l'efficacité
- Normes relatives aux systèmes de gestion

Mise en commun des pratiques exemplaires
- Il faut un processus d'inclusion, réunissant tous les groupes d'intervenants.
- Il faut un système d'échange de l'information.

Le temps presse
- Il faut commencer maintenant pour pouvoir profiter des avantages dans l'avenir.

Obtenir la participation des intervenants
- Commencer avec une approche claire et transparente pour obtenir leur engagement
- Analyser la rentabilité du projet pour le milieu des affaires
- Le financement

Séance de groupe n^{o} 1 : Besoins en matière de normalisation

THÈME 1 : Perspective juridique et réglementaire

L'objectif de cette séance était de déterminer les normes et les initiatives existantes et celles qu'il faut créer pour mettre en place une stratégie canadienne de normalisation à l'appui de la protection de la vie privée, d'un point de vue juridique et réglementaire.

La *Loi sur la protection des renseignements*

existing and needed standards and initiatives required to establish a Canadian Standardization Strategy to Support Privacy from a legal and regulatory perspective.

PIPEDA is perceived to be a good and reasonable law setting out what needs to occur in the private sector. What is needed in support of PIPEDA (and similar provincial requirements) is:

- Guidance on application, especially to small and medium enterprise;
- Clarity on sanctions for non-compliance;
- Clear requirements for breach notification;
- Consistency in application of laws/regulations across Canada;
- Best practices for different sectors and industries; and
- Details on limits of outsourcing to firms beyond Canada's laws.

Most of these identified gaps can be addressed through the standardization process with additional resources required to engage those delivering services where privacy needs to be respected. Some of the gaps will need additional regulation to be filled.

The federal law on privacy was recognized as being in need of revision in light of the rapidly increasing ease of acquiring personal information from individuals and the ease with which information can be shared and aggregated – with unintended consequences affecting the integrity of the data and the privacy of the individual.

The increasing number of IT offerings to assist government in their obligations was noted, along with the lack of clarity over whether the emphasis is on data security or the privacy rights of the individual.

The standards system was perceived of potential use to government provided there was a desire to have all affected parties involved in the discussions to revise the ATIP.

STREAM 2: Commercial and Product Vendors

A need was felt for standards to both support conformance to legislation as well as to provide suites of best practices for different industries and commercial exchanges.

personnels et les documents électroniques (*LPRPDÉ*) est considérée comme une loi utile et raisonnable, qui fixe ce qui doit se produire dans le secteur privé. Pour appuyer la *LPRPDÉ* (et les lois provinciales similaires), il faut :

- des lignes directrices relatives à l'application, surtout pour les petites et moyennes entreprises;
- des sanctions claires en cas de non-conformité;
- des exigences claires concernant la notification des brèches dans la protection des données;
- l'uniformité à l'échelle du Canada dans l'application des lois et des règlements;
- des pratiques exemplaires pour les divers secteurs et industries;
- des détails sur les limites de l'impartition aux entreprises qui ne sont pas soumises aux lois canadiennes.

La plupart des lacunes observées peuvent être comblées au moyen du processus de normalisation. Il faudra se doter de ressources additionnelles pour mettre à contribution les fournisseurs de services là où il faut protéger la vie privée. Certaines de ces lacunes ne seront corrigées qu'au moyen de règlements supplémentaires.

On a reconnu que la loi fédérale relative à la protection de la vie privée devait être revue lorsqu'on a constaté à quel point il devenait facile d'obtenir des renseignements personnels sur les gens et d'échanger et de regrouper ces informations ─ ce qui entraîne des répercussions non intentionnelles sur l'intégrité des données et la vie privée des personnes.

On a noté que les technologies de l'information visant à aider le gouvernement à remplir ses obligations se multiplient. Toutefois, on ignore si l'accent est mis sur la sécurité des données ou sur le droit des personnes à la vie privée.

On considère que le système de normes pourrait être utile au gouvernement, pourvu qu'il y ait une volonté de faire participer toutes les parties intéressées aux discussions menant à la révision de l'AIPRP.

A variety of complementary ideas were indicated:

- Privacy Impact Assessment as an important factor in any Risk Management/Assessment activity
- A common data collection policy is needed that addresses a variety of risk levels
- The control of transfer of data needs to be in the hands of the party whose information is being transferred/shared
- The intrusiveness of data collected needs to match the need for the data
- Clear rules are required for what data may be collected, the use of that data, the disclosure/ sharing/sale of that data, the protection of that data (security), the transfer of that data – in particular to jurisdictions outside where the data was collected, and the disposal of the data

This needs to be accomplished while taking into account the limited capacity/resources of SMEs to understand what is needed and to implement appropriate policies and protocols.

STREAM 3: Services and Product Users

The objective of this session was to identify the existing and needed standards and initiatives required to establish a Canadian Standardization Strategy to Support Privacy from a services and product user perspective.

Service and product users include a wide range of stakeholders from private citizens to the Canadian government. It must be scalable to be implemented by small, medium and large enterprises. This is particularly important as governments and large organizations look more to outsourcing services, including data collection and management services. It was discussed that the focus was on the protection of personal information of individuals and not on company-related information. The key elements for the federal government were the outsourcing of data management that may involve personal information to the private sector.

From the federal government perspective, this requirement was how to communicate the policies to the contractors and provide the ability to enforce these policies. This should be done in a way that is clear and explicit for the contractors. Standards would be very useful in this area as it has been in the IT and security areas. The ability to

THÈME 2 : Fournisseurs et vendeurs

Les participants ont jugé qu'il était nécessaire de se doter de normes pour appuyer la conformité à la loi et pour proposer un ensemble de pratiques exemplaires aux différentes industries et aux entreprises qui se livrent à des échanges commerciaux.

Plusieurs idées complémentaires ont été formulées :

- L'évaluation des facteurs relatifs à la vie privée est un élément important de toute activité de gestion ou d'évaluation du risque;
- Il faut se doter d'une politique commune de collecte des données qui s'adapte à une variété de niveaux de risque;
- Le contrôle du transfert des données doit appartenir à l'entité dont l'information est transférée ou échangée;
- Le niveau d'ingérence associé à la collecte des données doit correspondre aux besoins;
- Il faut des règles claires pour déterminer les données à recueillir, l'utilisation de ces données, le droit de communiquer, d'échanger ou de vendre ces données, la façon de protéger ces données (sécurité), si on peut transférer ces données ─ en particulier à des juridictions extérieures à celles où les données ont été recueillies ─ et l'élimination des données.

Il faut accomplir cela tout en tenant compte du fait que les PME ont des capacités et des ressources limitées pour comprendre ce qu'il faut faire et mettre en œuvre les politiques et protocoles appropriés.

THÈME 3 : Utilisateurs des produits et services

L'objectif de cette séance était de déterminer les normes et les initiatives existantes et celles qu'il faut créer pour mettre en place une stratégie canadienne de normalisation à l'appui de la protection de la vie privée, du point de vue des utilisateurs des produits et services.

Les utilisateurs des produits et services comprennent un large éventail d'intervenants, depuis les citoyens jusqu'au gouvernement canadien. Les solutions doivent être applicables à des échelles variables afin de pouvoir être mises

quote the standards to vendors in a contract was invaluable.

Another area of concern was where there was a stream of data; there may be policy implications beyond just privacy, such as encompassing security and IT. There was a sense that participants would rather see a more general or comprehensive standard that encompassed these requirements rather than a myriad of standards covering specific requirements. The discussion led to the notion that standards could help explain goals, uses and requirements. Privacy cannot be dealt with in isolation. It was identified that one set of standards need to be developed rather than disjointed standards for each area.

Liability was raised as an issue. It was pointed out that liability ultimately comes back to the individual who is wronged. However, through such practices as ID theft or data mining, the individual may be financially or morally ruined and must seek compensation or restitution independently. Also, the question of the obligation of an organization to report the discovery of the problem was discussed. The need for safeguards and requirements of data stores such as logs to be verifiable (using standardized date formats for example) were identified. This issue can bee addressed contractually, through certification or other legal means. However, this requires a commonly-understood "language" between and among the various players.

The problems associated with the collection of data by medical researchers, especially where the collection involves more detail than the commonly-accepted "basic" information was identified. Researchers are faced with a myriad of policies, legislations, and regulations across Canada that are not harmonized. The need for a "roadmap" to navigate these policies and this plethora of legislation was identified.

Improving awareness in the area of privacy is also critical. The harmonization of provincial and federal regulations is required so that users can develop products based on one set of regulations. The unique needs of various groups need to be identified.

STREAM 4: Consumer and Public Interest

The objective of this session was to identify the

en œuvre par des entreprises petites, moyennes ou grandes. Cela est particulièrement important parce que les gouvernements et les grandes organisations recourent davantage à l'impartition, notamment pour les services de collecte et de gestion des données. La discussion a porté sur le fait qu'on devait se centrer sur la protection des renseignements personnels des individus et non sur les informations liées aux entreprises. En ce qui concerne le gouvernement fédéral, les éléments clés étaient l'impartition au secteur privé de la gestion de données susceptibles de comprendre des renseignements personnels.

Du point de vue de l'administration fédérale, le besoin concernait la manière de communiquer la politique aux entrepreneurs et de se doter de la capacité d'assurer l'application de ces politiques. Cela devrait être accompli d'une façon qui soit claire et explicite pour les entrepreneurs. Les normes seraient très utiles dans ce domaine, comme elles l'ont été dans les secteurs de la TI et de la sécurité. La capacité d'intégrer des normes aux contrats conclus avec les fournisseurs n'a pas de prix.

On s'est aussi penché sur le flux de données pour lequel il peut y avoir des incidences stratégiques qui dépassent la vie privée, comme des incidences liées à la sécurité et à la TI. En général, les participants ont dit préférer une norme générale et intégrante qui couvre l'ensemble des exigences à une myriade de normes traitant chacune d'exigences précises. La discussion a porté sur l'impression que les normes pouvaient contribuer à expliquer les buts, les utilisations et les exigences. La protection de la vie privée ne peut pas être traitée isolément. On a conclu qu'il fallait élaborer un ensemble de normes plutôt que des normes distinctes pour chaque domaine.

On a soulevé le problème de la responsabilité. On a souligné qu'en définitive, c'est la personne victime de la fraude qui est tenue responsable. Pourtant, à la suite d'un vol d'identité ou du forage des données, la personne visée peut être démolie, tant sur le plan financier que moral, et doit chercher une compensation ou une restitution de manière indépendante. On a aussi parlé de l'obligation de l'organisation de signaler la découverte d'un problème. On a déterminé qu'il était nécessaire de se doter de mesures de protection ainsi que de systèmes de stockage des données, comme les journaux d'exploitation, qui

existing and needed standards and initiatives required to establish a Canadian Standardization Strategy to Support Privacy from a consumer and public interest perspective.

While the breakout group was made up of individuals from a range of stakeholder interests, there was strong agreement that any standards strategy development and standards work in the area of privacy needed to take a very inclusive approach, where the interests of all stakeholders were represented. In particular, it was noted that resources may need to be identified to ensure that consumer voice is represented and to build the capacity of the consumer constituency in Canada on this subject.

In terms of existing standards and legislation, there was general agreement that PIPEDA and provincial laws, based on the CSA Model Code, provide the essential principles for privacy protection in Canada. It was noted that while many consumers feel that their privacy is eroding, they may be willing to give up personal information as long as they are assured that their information will be protected and that there will be consequences for non-compliance. A recent study by the University of Ottawa has shown that there is widespread non-compliance with PIPEDA.

Industry codes such as the Canadian Marketing Association Privacy Code are useful in providing consumer assurance, but it is important to have direct consumer involvement in the development of these codes and public review of the draft codes. Other initiatives that should be reviewed include: OECD's initiative to harmonize security and privacy principles, Generally Accepted Privacy Principles (GAPP from the Accounting Sector), Short Notice as outlined in the Berlin Memorandum, and CEN audit standards and best practice guidelines.

Gaps in standards and legislation should be identified through risk assessment – what are the risks to consumers? While standards have been developed to cover security of information, the other 9 principles in PIPEDA (based on the CSA Code) have not been well developed and there is a need to develop more specific, clear implementation guidelines and best practices for the other principles, which would assist organizations with implementation. For example, it is difficult to make disclosure meaningful to consumers – more guidance is needed in this area. The issue of breach

soient vérifiables (grâce à des formats de données normalisés, par exemple). Ce problème peut être traité par contrats, par une certification ou par d'autres moyens législatifs. Il faudra cependant que les intervenants utilisent un « langage » commun.

On a cerné les problèmes associés à la collecte de données par les chercheurs en médecine, surtout là où la collecte exige plus de détails que ce qui est communément accepté. Les chercheurs sont aux prises avec une myriade de politiques, de lois et de règlements non harmonisés à l'échelle du Canada. Ils ont besoin d'une « feuille de route » pour gérer l'ensemble de ces politiques et de ces lois.

Il est aussi essentiel de sensibiliser davantage le public à la protection des renseignements personnels et de la vie privée. L'harmonisation des règlements provinciaux et fédéraux est nécessaire pour permettre aux utilisateurs d'élaborer des produits basés sur un ensemble unique de règlements. Il faut définir les besoins uniques des différents groupes.

THÈME 4 : Intérêts du public et des consommateurs

L'objectif de cette séance était de déterminer les normes et les initiatives existantes et celles qu'il faut créer pour mettre en place une stratégie canadienne de normalisation à l'appui de la protection de la vie privée, du point de vue du consommateur et du public.

Le groupe de discussion, bien que composé d'intervenants de différents secteurs, était d'avis que l'élaboration d'une stratégie de normalisation et les travaux sur les normes de protection de la vie privée devaient se faire de manière très inclusive, afin de tenir compte des intérêts de tous les intervenants. Il a souligné qu'il y aurait peut-être lieu de déterminer les ressources nécessaires pour veiller à la représentation des consommateurs et rehausser leur capacité à cet égard.

Quant aux normes et aux lois existantes, on s'entend pour dire que la *LPRPDÉ* et les lois provinciales, fondées sur le Code type de l'Association canadienne de normalisation (CSA), établissent les principes fondamentaux de protection de la vie privée au Canada. On a

notification was also raised a current gap in legislation. Any work on best practices needs to be supported with legal commentary.

Overall, the group was in support of a national standards strategy for privacy in Canada, building on existing standards, codes and legislation. A holistic approach was recommended, utilizing partnerships and engagement of all stakeholders.

Breakout Session 2: Standardization Solutions

STREAM 1: Role of Standards within Government Policy

The objective of this session was to identify solutions related to government policy for the needs identified in each of the following categories: 1) Legal and Regulatory, 2) Commercial and Product Vendors, 3) Services and 4) Product Users and Consumer and Public Interest.

It was generally agreed that PIPEDA is good principle-based legislation and what is missing is likely a number of guidelines about its interpretation. However, it was noted that these guidelines should offer a certain level of flexibility for businesses. A number of issues were raised with regards to Information Management laws. As an example, it was noted that the concept of identity theft may have different interpretations. A number of issues were raised with regards to the disclosure of personal information when a breach has occurred. It was felt that while a breach notification is a good idea, it should probably be handled differently depending on the nature of the personal information disclosed (i.e. medical versus financial).

The issue of data encryption was raised but it was not clear whether encrypted information is still considered personal information and apparently the government policy on this type of information is not well known.

It was generally agreed that having clear privacy legislation in a country helps in commercial transactions. It was also noted that Canadian legislation has a global impact on commerce.

constaté que même si les consommateurs ont l'impression que leur vie privée est de moins en moins protégée, ils sont prêts à fournir leurs renseignements personnels s'ils sont sûrs que l'information est protégée et qu'il y aura des conséquences dans les cas de non-conformité. Une étude récente réalisée par l'Université d'Ottawa a démontré que la non-conformité à la *LPRPDÉ* était courante.

Les codes de l'industrie, comme le Code de déontologie et Guides de conformité de l'Association canadienne du marketing (ACM), sont utiles pour rassurer les consommateurs, mais il est important que ceux-ci participent directement à l'élaboration de ces codes et à l'examen public des projets de codes. Parmi les initiatives à examiner figurent l'initiative de l'OCDE visant à uniformiser les principes de sécurité et de protection de la vie privée, les principes généralement reconnus de protection de la vie privée (GAPP du secteur comptable), le *Short Notice* du mémorandum de Berlin et les normes de vérification et directives sur les pratiques exemplaires du CEN.

On doit cerner les lacunes des normes et des lois grâce à une évaluation des risques – Quels sont les risques pour les consommateurs? Même si les normes ont été élaborées pour traiter de la protection des renseignements personnels, les neuf autres principes de la *LPRPDÉ* (basé sur le Code de la CSA) n'ont pas été adéquatement élaborés. Il faut élaborer des directives de mise en œuvre et des pratiques exemplaires précises et claires pour les autres principes, ce qui aiderait les organisations dans la mise en œuvre. Par exemple, il est difficile de faire en sorte que les consommateurs saisissent bien le sens et les implications d'une communication. Il faudra donc élaborer davantage de directives dans ce domaine. Le problème lié à la notification des brèches dans la protection des données a aussi été soulevé, car il ne fait pas l'objet d'une loi. Tous les travaux sur les pratiques exemplaires doivent être appuyés par un commentaire juridique.

Dans l'ensemble, le groupe appuie une stratégie nationale de normalisation en matière de protection de la vie privée qui pourra s'inspirer des normes, des lois et des codes existants. On recommande une approche holistique, ayant recours à des partenariats et à la participation des intervenants.

STREAM 2: Technical Standards, Tools, and Best Practices

The objective of this session was to identify potential solutions related to technical standards, tools, and best practice for the needs identified in each of the following categories: 1) Legal and Regulatory, 2) Commercial and Product Vendors, 3) Services and Product Users, and 4) Consumer and Public Interest.

It was estimated that 60-70% of the requirements needs to satisfy privacy already exist in other standards. However, there are some very different requirements that are not yet addressed in other standards (e.g. consent, usage permission). It was recommended to look at the existing public standards as a starting point and determine if they are adequate. Participants suggested standardizing the general privacy principles first, then developing a family of standards under each.

The desire to focus on the national level first was identified while taking into consideration what technical standards already exist at the international level. The development of a subcommittee to feed into the international process and work was recommended.

STREAM 3: Security Support for Privacy

The overarching need identified was the need to undertake a holistic approach to the blend of technology, policy and process addressing the full information life cycle from initial collection, use, disclosure, sharing, transfer, and disposal.

The results must be useful to SMEs – through targeted messages employing the information dissemination vectors normally used by SMEs, as well as inspections provided on a social basis, along the lines of fire hazard inspections.

There needs to be a clear and succinct description of the relation amongst privacy, accessibility and security.

To-date there has been much focus on security needs to protect technology from criminal elements; there are also other types of security needs that need to be addressed, such as ignorance and human error for person-to-person transactions, especially discussion of private details in a public space.

Discussion en atelier 2 : solutions de normalisation

THÈME 1 : Rôle des normes dans la politique gouvernementale

L'objectif de l'atelier était de trouver des solutions liées à la politique gouvernementale pour combler les besoins dans chacune des catégories suivantes : 1) la législation et la réglementation, 2) les fournisseurs et les vendeurs de produits, 3) les utilisateurs des produits et services et 4) l'intérêt des consommateurs et du grand public.

On s'entend généralement pour dire que la *LPRPDÉ* repose sur de bons principes et que ce qui lui fait défaut sont des lignes directrices sur son interprétation. Toutefois, on a observé que ces lignes directrices doivent être souples pour les entreprises. On a soulevé un certain nombre de questions sur les lois traitant de la gestion de l'information. Par exemple, on a observé que le concept de vol d'identité peut être interprété de diverses façons. Un certain nombre de questions ont été soulevées relativement à la communication de renseignements personnels lorsque survient une brèche dans la protection des données. Même si on estimait bonne l'idée d'une notification en cas de brèches, on était d'avis qu'il fallait probablement traiter l'affaire différemment selon la nature des renseignements personnels incorrectement communiqués (p. ex. renseignements médicaux ou financiers).

La question du chiffrement des données a été soulevée, mais on ignorait si l'information chiffrée appartenait encore à la catégorie des renseignements personnels et, apparemment, la politique gouvernementale sur ce type d'information n'est pas bien connue.

On était généralement d'accord pour dire qu'une législation claire sur le droit à la vie privée facilite les transactions commerciales dans un pays. On a également observé que la loi canadienne avait un effet sur le commerce mondial.

THÈME 2 : normes techniques, outils et pratiques exemplaires

L'objectif de l'atelier était de trouver des solutions possibles liées aux normes techniques, aux outils et aux pratiques exemplaires pour répondre aux besoins dans chacune des catégories suivantes : 1) la législation et la réglementation, 2) les

The inability of individuals to be aware of who accesses private data and for what reason is a major concern. There was support for the idea that individuals be alerted of every access to files containing private data.

An informational initiative to promote "Fair Information Practices" was seen as beneficial to both consumers and providers of services/goods to consumers.

STREAM 4: Verification, Audit and Conformity Assessment

The objective of this session was to identify potential solutions related to verification, audit and conformity assessment in each of the following categories: 1) Legal and Regulatory, 2) Commercial and Product Vendors, 3) Services and Product Users, and 4) Consumer and Public Interest.

In this breakout session there was general agreement that there was a need to evolve the area of verification and audits for privacy in Canada. There were a variety of opinions on the tools that are needed and the range of alternatives that should exist. Some members felt that any standards strategy for privacy needed to be based on nationally recognized consensus standards supported by accredited 3rd party conformity assessment programs. However, others in the group felt that verification could be achieved through self certification or through industry association programs for verification. Clearly, it would appear that there is a need for a continuum of options for verification and auditing, depending on the sector and the needs of stakeholders. For example, it would be helpful to develop self –assessment and internal audit checklists for small and medium enterprises. Some of these tools are being developed by Privacy Commissioners and by trade associations. It was also noted that 3rd party registrars are starting to offer audit services for the new ISO standard on Security Management and this experience should be evaluated /monitored to assess the value of this verification.

There was general concern that existing terms of reference for audits are poorly framed and in some cases not very robust. Every stakeholder has a different perspective on what is required. CEN has well developed audit tools and these should be considered for international or national application. Furthermore, trust marks or seals are

fournisseurs et les vendeurs de produits, 3) les utilisateurs des produits et services et 4) l'intérêt des consommateurs et du grand public.

On a estimé que 60 à 70 p. 100 des conditions nécessaires à la protection de la vie privée se trouvent déjà dans d'autres normes. Toutefois, certaines conditions très différentes ne sont pas encore remplies et ne sont pas abordées dans les autres normes (p. ex. le consentement, la permission d'utilisation). On a recommandé, pour commencer, d'examiner les normes publiques actuelles et de voir si elles sont appropriées. Les participants ont suggéré de normaliser d'abord les principes de protection de la vie privée, puis d'élaborer un ensemble de normes pour chacun de ces principes.

On a exprimé le désir de se concentrer d'abord sur l'échelon national tout en prenant en considération les normes techniques qui existent déjà à l'échelon international. On a recommandé la création d'un sous-comité pour participer aux travaux et au processus international.

THÈME 3 : soutien aux mesures de protection de la vie privée

Le besoin fondamental qui est ressorti est celui d'adopter une approche holistique face à l'éventail des technologies, des politiques et des processus associés au cycle de vie de l'information, de la collecte à l'élimination, en passant par l'utilisation, la communication, l'échange et le transfert.

Les résultats doivent être utiles aux PME – avec des messages ciblés employant les vecteurs de diffusion de l'information normalement utilisés par les PME, ainsi que des inspections axées sur l'aspect social et inspirées des inspections de prévention des incendies.

Il faut décrire succinctement et clairement la relation entre la protection de la vie privée, l'accessibilité et la sécurité.

À ce jour, on s'est surtout concentré sur les besoins de sécurité visant à protéger les ressources technologiques contre les éléments criminels; mais il faut également tenir compte d'autres d'autres types de besoins en matière de sécurité, comme l'ignorance et les erreurs humaines dans les transactions de personne à personne, en particulier pour les entretiens dans

not the total solution – they do not necessarily provide the consumer with required confidence or trust that their privacy has been protected. In light of recent breaches, consumers are looking for more assurance of compliance.

It was noted that in addition to audits and verification of privacy policies and procedures, there may be a need for personnel certification in this field. For example, the certification of privacy auditors or of engineers developing security systems may be appropriate. In the area of software applications, there are many providers but it is difficult at this stage to know if they meet privacy requirements. Verification and auditing would appear to have an increasing role to play as our data systems and information management structures become more complex, to ensure that privacy rights are assured.

The group had a lively discussion on the use of privacy impact assessments and the need for standardization of these tools. There were some who felt that these were not robust enough and some general standardized requirements may be required in this field. However, experience in Europe has shown that it may be better to simply have solid risk assessment practices, not to develop specific requirements for privacy. Guidance on the requirements for privacy impact assessments must come from Data Protection Commissioners, but could be provided through a voluntary standards solution.

* * *

un lieu public où il est question de détails privés.

L'une des principales causes de préoccupation se rapporte à l'incapacité des personnes de savoir qui a accès à leurs renseignements personnels et de connaître les raisons pour lesquelles on y a accès. Certains étaient d'avis qu'il fallait informer les gens chaque fois que quelqu'un consultait leurs renseignements personnels.

Une initiative d'information pour promouvoir des pratiques d'information équitables a été jugée utile aux consommateurs et aux fournisseurs de biens et de services.

THÈME 4 : vérification, contrôle et évaluation de la conformité

L'objectif de cet atelier était de trouver des solutions possibles liées à la vérification, au contrôle et à la vérification de la conformité dans chacune des catégories suivantes : 1) la législation et la réglementation, 2) les fournisseurs et les vendeurs de produits, 3) les utilisateurs de produits et services et 4) l'intérêt des consommateurs et du grand public.

Dans cette discussion en atelier, l'ensemble des participants ont convenu qu'il fallait améliorer le secteur de la vérification et du contrôle du point de vue de la protection des renseignements personnels au Canada. Ils ont exprimé divers points de vue sur les outils nécessaires et l'éventail des options qui devrait exister. Certains participants estimaient que les stratégies de protection de la vie privée devaient se fonder sur des normes nationales consensuelles soutenues par des programmes indépendants et accrédités d'évaluation de la conformité. Toutefois, d'autres membres étaient d'avis que la vérification pourrait se faire par autocertification ou au moyen des programmes de vérification des associations industrielles. Il apparaît clairement qu'on a besoin d'un ensemble d'options de vérification et de contrôle adaptées au secteur et aux besoins des intéressés. Par exemple, il serait utile de créer des listes de contrôle d'autoévaluation et de vérification interne pour les petites et moyennes entreprises. Certains de ces outils sont actuellement élaborés par les commissaires à la vie privée et par des associations professionnelles. On a aussi observé que des registraires indépendants commencent à offrir des services de vérification pour la nouvelle norme

ISO sur la gestion de la sécurité. Il faut évaluer et surveiller cette expérience pour connaître l'efficacité de cette vérification.

L'ensemble des participants se sont dits inquiets du fait que les paramètres de contrôle étaient mal définis et, dans certains cas, peu rigoureux. Chacun des intervenants avait un point de vue différent sur les mesures nécessaires. Le CEN a des outils de contrôle bien élaborés et il y aurait lieu d'envisager de les appliquer aux échelles internationale et nationale. En outre, les marques de confiance ou les sceaux ne sont pas la solution ultime, car ils ne rassurent pas les consommateurs et ne garantissent pas que leurs renseignements personnels seront protégés. Depuis les récents cas de brèches dans la protection des données, les consommateurs veulent davantage de garanties.

On a observé qu'en plus des contrôles et de la vérification des politiques et des procédures en matière de protection de la vie privée, il pourrait être nécessaire d'établir un processus de certification du personnel dans ce domaine. Par exemple, il pourrait être souhaitable de certifier les vérificateurs de la protection de la vie privée ou les ingénieurs qui élaborent des systèmes de sécurité. Dans le domaine des applications logicielles, il existe de nombreux fournisseurs, mais il est difficile pour l'instant de savoir s'ils respectent les exigences en matière de protection de la vie privée. La vérification et le contrôle semblent avoir un rôle de plus en plus grand à jouer dans la protection du droit à la vie privée compte tenu de la complexification grandissante des structures de gestion de l'information et des systèmes de données.

Le groupe a eu une discussion animée sur les évaluations des facteurs relatifs à la vie privée et la nécessité de normaliser ces outils. Certains participants étaient d'avis que ces outils n'étaient pas suffisamment rigoureux et qu'il faudrait procéder à une normalisation générale dans ce domaine. Toutefois, l'expérience européenne indique qu'il vaut peut-être mieux établir de solides pratiques d'évaluation des risques plutôt que d'élaborer des paramètres de protection de la vie privée. Les directives sur les exigences relatives aux évaluations des facteurs relatifs à la vie privée doivent venir des commissaires à la protection des données, mais pourraient provenir d'une solution axée sur l'adhésion facultative à des normes.

29E CONFÉRENCE INTERNATIONALE DES COMMISSAIRES
À LA PROTECTION DES DONNÉES ET DE LA VIE PRIVÉE

LES HORIZONS DE LA PROTECTION DE LA VIE PRIVÉE

TERRA INCOGNITA

PRIVACY HORIZONS

29TH INTERNATIONAL CONFERENCE OF
DATA PROTECTION AND PRIVACY COMMISSIONERS

Initiatives de sécurité au sein de l'Union internationale des télécommunications

Security Initiatives in the International Telecommunications Unions

Par/By:

Michael Harrop

Office of the Privacy Commissioner of Canada

Commissariat à la protection de la vie privée du Canada

Introduction

Dans un monde qui repose de plus en plus sur les communications électroniques et les données informatiques, les mesures de sécurité efficaces sont primordiales pour protéger les systèmes et les données que ceux-ci contiennent et traitent. Sans cette sécurité, toutes les données traitées électroniquement sont à risques. L'UIT-T vise essentiellement, par ses travaux, l'établissement d'une base solide pour l'élaboration et la mise en œuvre de produits et de services sûrs en veillant à ce que les normes de sécurité requises existent. Une sécurité efficace suppose aussi que les utilisateurs appliquent des pratiques informatiques fiables et se conforment aux exigences des politiques de sécurité locales. Dans cette optique, les milieux de la normalisation jouent un rôle de plus en plus important dans la promotion de la sécurité et des pratiques exemplaires.

Bien que les termes *sécurité* et *protection de la vie privée* soient souvent confondus et parfois employés de façon interchangeable, ils renvoient à des notions très différentes qu'il importe de distinguer. Par exemple, les mécanismes de sécurité peuvent concerner les moyens techniques requis pour protéger la vie privée (p. ex., en assurant une protection contre la communication, la modification ou la destruction non autorisées de renseignements sensibles), tandis que la protection de la vie privée englobe les considérations juridiques et sociologiques qui vont au-delà de la portée des mesures de sécurité. Ainsi, il est tout à fait possible que des renseignements personnels soient conservés de façon sécuritaire par une organisation, mais si celle-ci n'était pas autorisée au départ à recueillir l'information, il y a atteinte à la vie privée des personnes concernées. Cela dit, si les notions de « sécurité » et de « protection de la vie privée » diffèrent, elles ont un important point commun en ce sens que les services et les mécanismes de sécurité peuvent servir à renforcer la protection de la vie privée.

À titre de principal organisme international de normalisation des télécommunications, l'Union internationale des télécommunications (UIT) a instauré un certain nombre d'initiatives visant à répondre proactivement aux préoccupations liées à la sécurité des communications par le biais de ses propres commissions d'études et en collaboration avec d'autres organismes de normalisation.

Introduction

In a world that increasingly relies on electronic communications and electronically-stored data, effective security is of critical importance in protecting the functioning of systems and the data they process and hold. Without effective security, all electronically-processed data is at risk. One of the primary objectives of the ITU-T work is to provide a sound basis for the development and implementation of secure products and services by ensuring the needed security standards are available. Effective security also depends on users following safe computing practices and adhering to the requirements of local security policy. In support of this, the standards community is playing an increasing role in promoting security awareness and good practices.

Although the terms *security* and *privacy* are often confused and, not infrequently, used interchangeably, security and privacy are really quite different attributes and it is important to recognize the differences. For example, security mechanisms can address the technical measures needed to support privacy (e.g. by protecting against unauthorized disclosure, modification or destruction of sensitive information) but privacy extends to legal and sociological considerations that are beyond the scope of the security work. To illustrate this point further, it is entirely possible for personal information to be held quite security by an organization but if that organization should not have collected that information in the first place, the privacy of the person or persons that are the subject of that information has been violated. Nevertheless, although security and privacy are different attributes, there is an important intersection between these attributes in that security services and mechanisms can be used to support privacy.

As the leading international telecommunications standards body, the International Telecommunications Union (ITU) has established a number of initiatives to address communications security issues pro-actively within its own Study Groups and in collaboration with other standardization bodies.

The paper provides a brief overview of the ITU security-related standards work, and highlights some of the work of particular relevance to privacy protection. More detail is available via the web linkages provided for each of the topics.

Le présent document offre un bref aperçu du travail de l'UIT dans le domaine des normes de sécurité et met en lumière certaines des initiatives qui touchent particulièrement la protection des renseignements personnels. On peut obtenir de plus amples renseignements sur ces initiatives en cliquant sur les hyperliens fournis sous chaque rubrique.

Rôle de l'UIT-T

L'Union internationale des télécommunications (UIT) fait partie des institutions spécialisées de l'Organisation des Nations Unies. Le Secteur de la normalisation des télécommunications (UIT-T) sert de tribune aux gouvernements et organismes du secteur privé pour l'élaboration de normes relatives aux réseaux et aux services de télécommunications mondiaux.

On peut consulter un guide visant à mieux faire connaître l'UIT-T et son fonctionnement à l'adresse itu.int/ITU-T/promotion.

Les activités de l'UIT-T s'échelonnent sur un cycle de quatre ans (appelé *période d'études*) au cours duquel des *Recommandations* (c.-à-d., des normes UIT) sont élaborées et publiées. Les activités sont regroupées par sujet et confiées à des commissions d'études (CE). Au sein de chaque CE, les activités sont ensuite subdivisées en projets appelés *Questions*.

Le Tableau 1 fait état des 12 commissions d'études de l'UIT-T qui ont mené des activités liées à la sécurité au cours de la période d'études 2004-2008. Chacune de ces CE a nommé une personne-ressource chargée d'assurer la liaison en matière de sécurité. On peut trouver des précisions sur les activités des CE à l'adresse http://www.itu.int/ITU-T/studygroups/com17/security-questions.doc.

La CE 17 (*Sécurité, langages et logiciels de télécommunication*) est chargée des questions relatives à la sécurité des télécommunications et doit assurer la coordination entre toutes les commissions d'études à cet égard.

Voir le Tableau 1 à la page suivante

Role of the ITU-T

The International Telecommunication Union (ITU) is one of the specialized agencies within the United Nations system. The Telecommunication Standardization Sector (ITU-T) acts as a forum where governments and the private sector develop standards for global telecommunications networks and services.

A guide to the ITU-T and how it operates is available at itu.int/ITU-T/promotion

The ITU-T works on a four-year cycle (called a *Study Period*) during which *Recommendations* (i.e. ITU standards) are developed and published. The work is grouped by topic and assigned to Study Groups (SGs). Within each SG the work is subdivided into projects known as *Questions*.

Table 1 identifies the 12 Study Groups of the ITU-T that have been identified as having security-related activities during the 2004-2008 Study Period. Each of these SGs has appointed a specific contact for security liaison. More detailed information about the activities of each SG is available at:

http://www.itu.int/ITU-T/studygroups/com17/security-questions.doc

SG 17, *Security, Languages and Telecommunications Software,* has been designated the Lead Study Group for telecommunications security issues and has responsibility for security coordination across all Study Groups.

See Table 1 on the next page

Commission d'études 2 : Aspects opérationnels de la fourniture du service, réseaux et qualité de fonctionnement (Commission d'études responsable de la définition du service, du numérotage et de l'acheminement) (Commission d'études responsable des opérations de secours en cas de catastrophe et des alertes précoces) http://www.itu.int/ITU-T/studygroups/com02/index.asp
Commission d'études 4 : Gestion des télécommunications http://www.itu.int/ITU-T/studygroups/com04/index.asp
Commission d'études 5 : Protection contre les effets dus à l'environnement électromagnétique http://www.itu.int/ITU-T/studygroups/com05/index.asp
Commission d'études 6 : Installations extérieures et installations intérieures connexes http://www.itu.int/ITU-T/studygroups/com06/index.asp
Commission d'études 9 : Réseaux en câble intégrés à large bande et transmission télévisuelle et sonore http://www.itu.int/ITU-T/studygroups/com09/index.asp
Commission d'études 11 : Spécifications et protocoles de signalisation (Commission d'études responsable des conditions et des protocoles relatifs à la signalisation et aux réseaux intelligents) http://www.itu.int/ITU-T/studygroups/com11/index.asp
Commission d'études 12 : Qualité de fonctionnement et qualité de service http://www.itu.int/ITU-T/studygroups/com12/index.asp
Commission d'études 13 : Réseaux de prochaine génération (Commission d'études responsables des réseaux de prochaine génération et des questions liées aux satellites) http://www.itu.int/ITU-T/studygroups/com13/index.asp
Commission d'études 15 : Réseaux optiques et autres réseaux de transport http://www.itu.int/ITU-T/studygroups/com15/index.asp
Commission d'études 16 : Terminaux, systèmes et applications multimédias (Commission d'études responsable des terminaux, systèmes et applications multimédias et des applications ubiquistes (comme les soins de santé et les opérations commerciales en ligne) http://www.itu.int/ITU-T/studygroups/com16/index.asp
Commission d'études 17 : Sécurité, langages et logiciels de télécommunication (Commission d'études responsable de la sécurité des télécommunications) http://www.itu.int/ITU-T/studygroups/com17/index.asp
Commission d'études 19 : Réseaux de télécommunications mobiles http://www.itu.int/ITU-T/studygroups/com19/index.asp

Tableau 1 : Liste des CE de l'UIT-T qui ont des responsabilités en matière de sécurité

Study Group 2: Operational aspects of service provision, networks and performance (Lead Study Group for service definition, numbering and routing) (Lead Study Group for Disaster Relief/Early Warning) http://www.itu.int/ITU-T/studygroups/com02/index.asp
Study Group 4: Telecommunication management http://www.itu.int/ITU-T/studygroups/com04/index.asp
Study Group 5: Protection against electromagnetic environment effects http://www.itu.int/ITU-T/studygroups/com05/index.asp
Study Group 6 Outside Plant and related indoor installations http://www.itu.int/ITU-T/studygroups/com06/index.asp
Study Group 9 Integrated broadband cable networks and television and sound transmission http://www.itu.int/ITU-T/studygroups/com09/index.asp
Study Group 11 Signalling requirements and protocols (Lead Study Group on Signalling and Protocols and Intelligent Networks.) http://www.itu.int/ITU-T/studygroups/com11/index.asp
Study Group 12 Performance and quality of service http://www.itu.int/ITU-T/studygroups/com12/index.asp
Study Group 13 Next Generation Networks (Lead Study Group for NGN and satellite matters.) http://www.itu.int/ITU-T/studygroups/com13/index.asp
SG 15: Optical and other transport networks http://www.itu.int/ITU-T/studygroups/com15/index.asp
SG 16: Multimedia services, systems and terminals (Lead Study Group on multimedia terminals, systems and applications, and on ubiquitous applications (such as e-health and e-business)). http://www.itu.int/ITU-T/studygroups/com16/index.asp
Study Group 17: Security, languages and telecommunication software (Lead Study Group on telecommunication security) http://www.itu.int/ITU-T/studygroups/com17/index.asp
SG 19: Mobile Telecommunications Networks http://www.itu.int/ITU-T/studygroups/com19/index.asp

Table 1: ITU-T Study Groups with security responsibilities

Programme de travail de la Commission d'études 17

La CE 17 a établi quelques Questions relatives à la sécurité (c.-à-d., des projets) au cours de la présente période d'études. Ces Questions sont énumérées à la Figure 1. La plupart feront l'objet d'au moins une Recommandation (c.-à-d., norme). De plus, la CE compte un certain nombre de groupes spécialisés chargés d'examiner les enjeux liés à la sécurité. (Les groupes spécialisés ont plus de marge de manœuvre que les commissions d'études pour ce qui est de la participation et des méthodes de travail. Ils sont en effet constitués de manière à examiner rapidement les besoins de normalisation en évolution.) Les initiatives sont examinées plus en détail ci-après.

Voir la Figure 1 en annexe à la page 63

Examen plus approfondi d'Initiatives relatives à la sécurité de la CE 17

En tant que commission d'études responsable de la sécurité, la CE 17 mène un certain nombre d'initiatives dans le but de coordonner les travaux en matière de sécurité menés par l'UIT-T et de faire davantage connaître les activités dans le domaine.

Guide sur la sécurité dans les télécommunications

Notre publication intitulée *Sécurité dans les télécommunications et la technologie de l'information* donne un aperçu des enjeux et de la mise en application des recommandations de l'UTI pour la sécurité dans les télécommunications. Elle comprend un résumé de chaque recommandation liée à la sécurité et est disponible sur Internet ainsi que sur support papier. On peut la consulter à l'adresse :

http://www.itu.int/dms_pub/itu-t/opb/hdb/T-HDB-SEC.03-2006-PDF-F.pdf

Compendium sur la sécurité

Un compendium en trois parties sur la sécurité a été élaboré, qui comporte un catalogue des recommandations approuvées par l'UIT-T concernant la sécurité dans les

Study Group 17 Program of Work

SG 17 has established a number of security-related Questions (i.e. projects) in the current Study Period. These are illustrated in Figure 1. Most of the Questions will result in one or more Recommendations (i.e. standards). In addition, SG17 has a number of Focus Groups examining security-related issues. (Focus Groups have greater flexibility than SGs in terms of participation and working methods. They are established to give rapid consideration to evolving standardization needs.) These initiatives are reviewed in greater detail below

See Figure 1 in the Appendix on page 63

A Closer look at some of the SG 17 Security Initiatives

As the Lead Study Group for security, SG 17 is engaged in a number of initiatives in to coordinate security efforts across the ITU-T and to raise awareness about our security activities.

Telecommunications Security Guide

Our publication *Security in Telecommunications and Information Technology* provides an overview of issues and the deployment of existing ITU Recommendations for secure telecommunications. The manual includes a brief summary of each security-related recommendation and is available online as well as in hard copy format. The online version is available at:

http://www.itu.int/itudoc/itu-t/86435.html

Security Compendium

A three-part Security Compendium has been developed comprising: a catalogue of approved ITU-T Recommendations related to Telecommunication Security; approved ITU-T security definitions; and a listing of ITU-T security-related Questions. The Compendium is on-line as follows:

Approved Recommendations:
http://www.itu.int/ITU-T/studygroups/com17/cat005.doc
Approved definitions:
http://www.itu.int/ITU-T/studygroups/com17/def005.doc

télécommunications; des définitions de la sécurité approuvées par l'UIT-T; et une liste des Questions relatives à la sécurité de l'UIT-T. On peut consulter le compendium aux adresses suivantes :

Recommandations approuvées :
http://www.itu.int/ITU-T/studygroups/com17/cat005.doc
Définitions approuvées :
http://www.itu.int/ITU-T/studygroups/com17/def005.doc
Questions relatives à la sécurité :
http://www.itu.int/ITU-T/studygroups/com17/security-questions.doc

Feuille de route sur la sécurité

Bien que de nombreux travaux soient en cours et qu'un bon nombre de normes de sécurité aient été mises au point par des organisations internationales, il n'est pas facile pour les utilisateurs (voire les concepteurs) de normes de savoir s'il existe une norme de sécurité pour tel ou tel problème. On a en effet tendance, même chez les organismes de normalisation, à classer les normes de sécurité avec les autres normes relatives à la TI plutôt que de les organiser en fonction du sujet qu'elles abordent. Pour tenter de régler ce problème, la CE 17 a élaboré une feuille de route des normes de sécurité en vigueur.

La feuille de route, qui est en cours d'élaboration, dresse la liste des normes de sécurité en vigueur et terminées, des normes en voie d'élaboration et des domaines où des normes s'imposeraient, mais dont l'élaboration n'a pas été entreprise. Les normes sont classées en fonction de l'élément de sécurité qui est abordé (p. ex., directive d'ordre général, biométrique, politique, etc.). La feuille de route comprend les Recommandations de l'UIT-T et les normes et les travaux d'autres organismes de normalisation officiels et non officiels internationaux et régionaux. Elle vise à contribuer à la coordination des activités de normalisation en matière de sécurité en offrant un sommaire à jour des travaux qui ont pris fin ou qui sont en cours et en indiquant les principales organisations participant ou ayant participé aux travaux. En sachant quels éléments ont déjà été abordés ou sont en voie de l'être, on pourra éviter le double emploi et relever les lacunes. Un nouveau volet s'est récemment ajouté à la feuille de route, portant sur les pratiques exemplaires reconnues.

La version actuelle de la feuille de route couvre les normes de sécurité suivantes : UIT-T, ISO/CEI

Security-related Questions:
http://www.itu.int/ITU-T/studygroups/com17/security-questions.doc

Security Roadmap

Although a great deal of work is in progress and many security standards have been developed by international organizations, it is not easy for standards users (or even developers) to determine precisely what security standards already exist. Even within standards development organizations, security standards tend to be listed along with other IT standards, rather than being classified in terms of the particular aspects of security being addressed. To try to address this problem, SG 17 has developed a Roadmap of existing security standards.

The Roadmap, which is a work-in-progress, identifies existing completed security standards, standards in development, and areas where a need for standards has been identified but where work has not yet been initiated. Standards are listed under the particular aspect of security that they address (e.g. general security guidance, biometrics, security policy etc). The Roadmap includes not only ITU-T Recommendations but also the standards and work of other formal and informal regional and international standards development organizations. It is hoped that the Roadmap will contribute to the coordination of security standardization activities by providing an up-to-date summary of work that has been completed and work that is in progress, as well as identifying the major organizations participating in this work. By knowing what has been done already, and what work is in progress, it will be possible to avoid duplication of effort and also to identify gaps that need attention. A new part has recently been added to the Roadmap to cover recognized good practices.

The current version of this Roadmap covers the security standards of ITU-T, ISO/IEC JTC 1, IETF, IEEE, ATIS, ETSI and OASIS.

The Roadmap is available at:
http://www.itu.int/ITU-T/studygroups/com17/ict/index.html

JTC 1, IETF, IEEE, ATIS, Institut européen des normes de télécommunication et OASIS.

On peut consulter la Feuille de route (en anglais seulement) à l'adresse : http://www.itu.int/ITU-T/studygroups/com17/ict/index.html

Groupe spécialisé sur la gestion de l'identité (FG IdM)

En décembre 2006, la CE 17 de l'UIT-T et le projet IST Daidalos de l'Union européenne ont tenu un atelier intitulé *Identité numérique dans le contexte des réseaux de prochaine génération*. La rencontre visait à examiner les diverses approches concernant l'identité numérique, analyser les lacunes dans les normes contemporaines, recenser les défis qui se poseront et définir les buts communs qui guideront les travaux menés dans le cadre de différents projets et par les organisations de normalisation.

On trouvera des précisions sur l'atelier, de même qu'un compte rendu de celui-ci (en anglais seulement) à l'adresse : http://www.itu.int/ITU-T/worksem/ngn/200612/index.html

L'atelier a été jugé opportun et utile et a donné lieu à une réunion de suivi visant à répondre à certaines des questions ayant été soulevées. Les participants ont également jugé nécessaire l'adoption d'un mécanisme de coordination. Les discussions se sont poursuivies après l'atelier et ont entraîné la création du Groupe spécialisé de la CE 17 sur la gestion de l'identité.

Le Groupe spécialisé a pour principal objectif de faciliter l'élaboration d'un cadre général pour la gestion de l'identité en favorisant la participation de tous les spécialistes des télécommunications et des technologies de l'information et de communication dans le domaine de la gestion de l'identité.

Il vise aussi à :

(a) établir une liste à jour des organismes, forums et consortiums de normalisation œuvrant dans le domaine de la gestion de l'identité, y compris l'information sur leurs activités et leurs documents dans le contexte de la gestion de l'identité;
(b) mener une analyse globale des besoins et des capacités en matière de gestion de

Focus Group on Identity Management (FG IdM)

In December 2006 ITU-T SG 17 and the European Union IST Daidalos Project held a workshop entitled *Digital Identity for Next Generation Networks*. Workshop objectives were to investigate different approaches digital identity, analyze gaps in today's standards, identify future challenges and find common goals which will provide direction to the work currently being undertaken in the different projects and standards development organizations.

Details on the workshop and the results are documented at http://www.itu.int/ITU-T/worksem/ngn/200612/index.html

The workshop was considered as timely and useful, and resulted in a follow-up meeting to answer some of the questions raised. The need for a coordination mechanism was also seen as necessary. Discussions continued after the workshop and resulted in the establishment of an SG 17 Focus Group on Identity Management.

The overall objective of the Focus Group is to facilitate the development of a generic Identity Management framework, by fostering participation of all telecommunications and ICT experts on Identity Management.

The objectives include:

(a) Establishing a living list of standards bodies, fora, and consortia dealing with Identity Management, including information concerning their activities and documents in the context of an IdM framework;
(b) Conducting a global analysis on IdM requirements and capabilities;
(c) Developing a set of IdM telecommunications/ICT use cases that can be used to derive requirements; and
(d) Identifying new standards work that ITU-T SGs and other SDOs should undertake.

The Focus Group is attracting wide participation and interest and membership is open to ITU Member States, Sector Members and Associates as well as any individual from an ITU member country willing to contribute to the work. For latest results and more information please see: http://www.itu.int/ITU-T/studygroups/com17/fgidm/index.html

l'identité;

(c) élaborer un ensemble de cas d'utilisation des télécommunications et des technologies de l'information et de communication pour la gestion de l'identité susceptibles d'aider dans la définition des besoins;

(d) définir de nouvelles activités de normalisation que devraient entreprendre des commissions d'études de l'UIT-T et autres organismes de normalisation.

Le Groupe spécialisé attire un grand nombre de participants et suscite un vif intérêt. La participation est ouverte aux États membres, aux Membres de Secteur et aux Associés de l'UIT ainsi qu'à toute personne issue d'un pays membre de l'UIT qui souhaite contribuer aux travaux. Pour obtenir les plus récentes nouvelles et de plus amples renseignements, consulter (en anglais seulement) :

http://www.itu.int/ITU-T/studygroups/com17/fgidm/index.html

Recommandations liées à la sécurité

Une cinquantaine de recommandations sur la sécurité sont en voie d'élaboration. On en trouvera un résumé (en anglais seulement) à l'adresse : http://www.itu.int/ITU-T/studygroups/com17/sg17final-summaries.doc

Renseignements supplémentaires

Le présent document ne représente qu'un aperçu des activités menées par l'UIT-T en matière de sécurité. On trouvera une présentation beaucoup plus détaillée à l'adresse http://www.itu.int/ITU-T/special-projects/security/presentations/Telecommunication_Security.ppt

Sommaire

Des mesures de sécurité efficaces sont essentielles pour assurer la confidentialité, l'intégrité et l'authenticité de l'information, éléments clés dans le contexte de la protection de la vie privée. L'UIT-T mène un programme d'action ambitieux concernant tous les aspects de la sécurité des télécommunications. La majeure partie de ces activités contribueront à la protection de la vie privée des personnes et des organisations.

Security-related Recommendations

Approximately 50 security recommendations are currently under development. A summary of these Recommendations may be found at: http://www.itu.int/ITU-T/studygroups/com17/sg17final-summaries.doc

Further information

This paper presents only a brief overview of the ITU-T security work. A considerably more detailed presentation is available at http://www.itu.int/ITU-T/special-projects/security/presentations/Telecommunication_Security.ppt

Summary

Effective security is vital to protect the confidentiality, integrity and authenticity of information, all of which are of concern in the context of privacy. The ITU-T is pursuing an ambitious program of work directed towards all facets of telecommunications security. Much of this work will contribute to the protection of individual and organizational privacy.

* * *

Annexe / Appendix

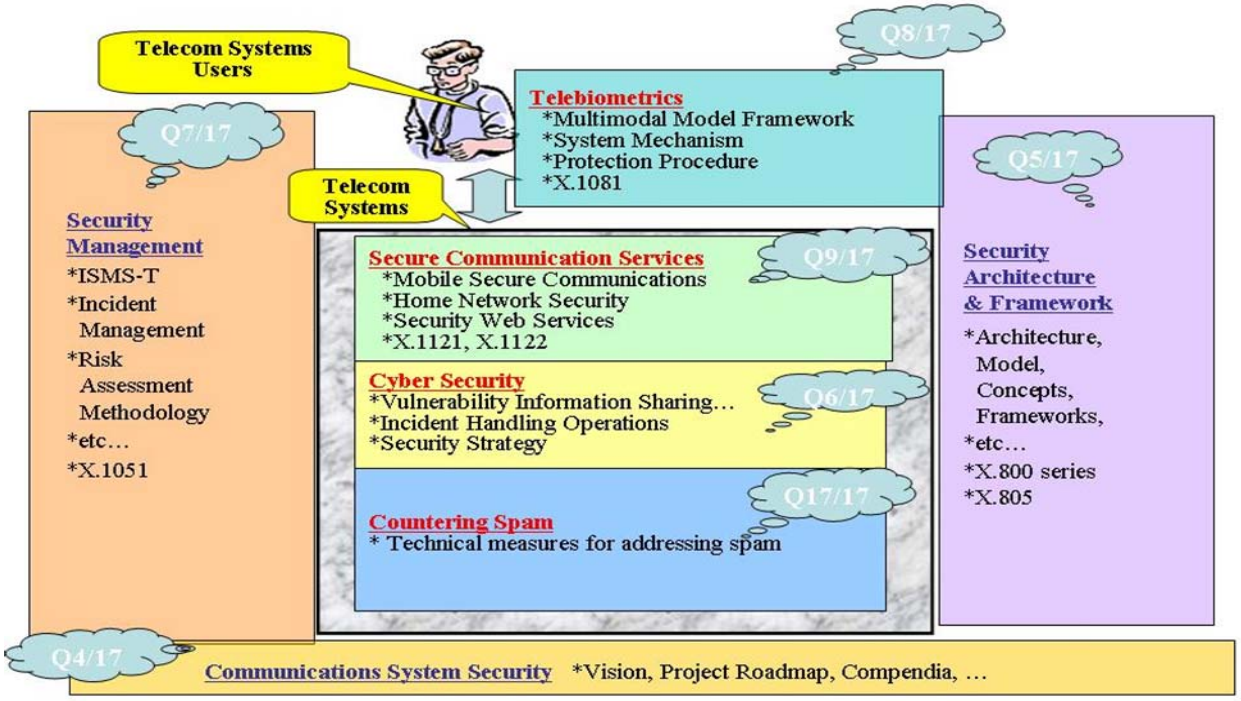

Figure 1: SG 17 Security Questions (2004-2008)

Figure 1 : Questions relatives à la sécurité de la CE 17 (2004-2008)

Traduction de la figure 1

Bulle jaune du haut = **Utilisateurs des systèmes de télécommunication**

Carré turquoise (centre + haut) = **Télébiométrique**
- Cadre de modèle multimode
- Mécanisme de système
- Procédure de protection
- X.1081

Carré Orange (gauche) = **Gestion de la sécurité**
- SGSI-T
- Gestion des incidents
- Méthode d'évaluation des risques
- Etc.
- X.1051

Bulle jaune du bas = **Systèmes de télécommunication**

Carré vert (centre + haut) = **Services de communication sûrs**
- Communications mobiles fiables
- Sécurité du réseau local
- Sécurité des services Web
- X.1121, X.1122

Carré jaune (centre + milieu) = **Cybersécurité**
- Échange d'information sur la vulnérabilité
- Opérations de traitement des incidents
- Stratégie en matière de sécurité

Carré bleu (centre + bas) = **Lutte contre les pourriels**
- Mesures techniques contre les pourriels

Carré mauve (droite) = **Architecture et cadre de sécurité**
- Architecture
- Modèle
- Notions
- Cadres
- Etc.
- Série X.800
- X.805

Encadré ocre (centre + bas) = **Sécurité des systèmes de communication**

29E CONFÉRENCE INTERNATIONALE DES COMMISSAIRES
À LA PROTECTION DES DONNÉES ET DE LA VIE PRIVÉE

LES HORIZONS DE LA PROTECTION DE LA VIE PRIVÉE

TERRA INCOGNITA

PRIVACY HORIZONS

29TH INTERNATIONAL CONFERENCE OF
DATA PROTECTION AND PRIVACY COMMISSIONERS

Atelier stratégique canadien sur les normes de protection de la vie privée
Séance d'information de l'ISO/CEI JTC 1
2 février 2007

Canadian Privacy Standards Strategy Workshop
ISO/IEC JTC 1 Briefing
February 2, 2007

Office of the Privacy Commissioner of Canada
Commissariat à la protection de la vie privée du Canada

Ndt : La présence d'un astérisque (*) suivant les titres dans ce texte et dans les annexes signifie qu'il s'agit d'une traduction, et donc d'un titre officieux (ils sont suivis de la mention « Titre manque » dans le site Web de l'ISO au 6 février 2007).

Le 2 février 2007

Le Comité technique des technologies de l'information (JTC 1) de l'ISO et de la CEI a pour mission d'élaborer des « normes de base » dans le domaine des technologies de l'information et des communications (TIC). L'expression « normes de base » désigne les normes dont d'autres organismes d'élaboration de normes affiliés ou non à l'ISO et à la CEI peuvent s'inspirer pour élaborer des normes plus spécifiques, propres aux domaines ou applications qui les intéressent concrètement. Le JTC 1 joue donc un rôle tout particulier dans le milieu de la normalisation, 30 % de ses clients étant d'autres organismes d'élaboration de normes. C'est ce qui explique, ne serait-ce qu'en partie, pourquoi les normes élaborées par le JTC 1 revêtent une telle importance.

Dans cet esprit, le JTC 1 et ses sous-comités (SC) doivent toujours envisager les pires éventualités à l'heure d'élaborer des normes. Ce n'est qu'ainsi qu'ils pourront avoir la certitude que ces normes trouveront une application et une utilité dans n'importe quel environnement. Pour ne citer qu'un exemple, l'ISO/CEI JTC 1/SC 27, qui s'occupe d'élaborer des normes relatives à la sécurité des technologies de l'information, doit invariablement veiller à ce que ces normes puissent fonctionner dans un environnement « hostile ». D'autres comités techniques et sous-comités relevant de l'ISO et de la CEI ne doivent pas nécessairement travailler dans un régime de contraintes aussi rigoureux, et les comités qui élaborent des normes dans un domaine d'activités spécifique peuvent opter pour des exigences plus malléables qui s'adaptent mieux à leur domaine d'intérêt. Ainsi, ils peuvent prendre une norme du JTC 1 et en « atténuer » les exigences pour mieux l'adapter à leur domaine, tout en ne perdant pas de vue que leur norme ne pourra donc pas nécessairement s'appliquer au domaine généralisé.

En ce moment, le JTC 1 comprend six sous-comités (SC) consacrés à l'élaboration de normes relatives à la protection de la vie privée, à savoir :

- ISO/CEI JTC 1/SC 17 – Identification des

2 Feb. 2007

ISO/IEC JTC 1 is tasked with developing "Base Standards" in the field of Information and Communications Technology (ICT). The term "Base Standards" means standards that other standards developers both inside and outside ISO and IEC can use to develop domain and application specific standards. This means that JTC 1 is unique within the standards world, in-so-much-as 30% of its customers are other standards developers. This is one of the reasons why JTC 1 standards are so important.

As consequence of the above, JTC 1 and its Sub Committees (SCs) must always consider the worst case scenario when developing its standards in order to ensure that those standards will be applicable and usable in any environment. As an example, ISO/IEC JTC 1/SC 27 which develops standards for security, must always develop those standards to work in a "hostile" environment. Some other Technical Committees and SCs within ISO and IEC do not have to work under such strict constraints, and those committees developing standards for a specific business domain may select less stringent requirements more appropriate to their domain. They can thus take a JTC 1 standard and "soften" the requirements thus making it more applicable to their domain, always bearing in mind that in so doing, their standard may not be applicable to the generalized domain.

JTC 1 currently has six Sub-Committees (SCs) developing standards related to Privacy. The SCs are:

- ISO/IEC JTC 1/SC 17 – Cards and Personal Identification,
- ISO/IEC JTC 1/SC 27 – IT Security Techniques,
- ISO/IEC JTC 1/SC 31 – Automatic Identification and Data Capture Techniques (RFID),
- ISO/IEC JTC 1/SC 32 – Data Management and Interchange,
- ISO/IEC JTC 1/SC 36 – Information Technology for Learning, Education & Training, and
- ISO/IEC JTC 1/SC 37 – Biometrics.

Brief details of their relevant published standards, work currently under development and planed work is provided in separate briefs for each SC, see the annexes to this document.

cartes et des personnes;
- ISO/CEI JTC 1/SC 27 – Techniques de sécurité des technologies de l'information;
- ISO/CEI JTC 1/SC 31 – Techniques d'identification et de captage automatique des données (RFID);
- ISO/CEI JTC 1/SC 32 – Gestion et échange des données;
- ISO/CEI JTC 1/SC 36 – Technologies pour l'éducation, la formation et l'apprentissage;
- ISO/CEI JTC 1/SC 37 – Biométrie.

On trouvera dans les annexes du présent document quelques précisions sur les normes publiées, les projets en cours et les travaux prévus pour chacun des sous-comités.

Le JTC 1 a adopté une résolution visant à confier au SC 27 tous les travaux futurs sur les normes de protection de la vie privée qui ne s'inscrivent pas déjà dans l'un des programmes de travail des autres cinq comités. Tout en rappelant que le Canada appuie les travaux que le SC 27 est en train d'effectuer pour l'élaboration de normes de protection de la vie privée auxquels il participe d'ailleurs activement, il estime et affirme qu'il est inapproprié que le SC 27 se fasse confier l'élaboration d'autres normes dans ce contexte, notamment en ce qui a trait aux bases de données ou aux systèmes d'exploitation. En ce moment, on estime que les normes relatives à la protection de la vie privée représentent environ 20 % de la totalité des normes requises à ce chapitre. On estime également que les travaux en cours chez d'autres SC du JTC 1 représentent 10 % de plus par rapport au total requis. Quant à confier au SC 27 les 70 % restants des travaux de normalisation requis, qui ne se rapportent pas à la protection de la vie privée, voilà longtemps déjà que le Canada déplore la démarche, criant à l'anathème.

Depuis les cinq dernières années, le Canada n'a eu de cesse que de demander au JTC 1 de constituer un SC exclusivement consacré aux technologies de protection de la vie privée. Or, pour l'instant, cette demande est tombée dans le vide. Le principal inconvénient résiderait dans l'impossibilité de financer un secrétariat pour un tel SC. Il existe suffisamment d'organismes nationaux qui ont exprimé leur intérêt et leur volonté de participer à un tel SC, en revanche aucun d'eux ne semble disposé à financer le secrétariat.

Currently, JTC 1 has a resolution directing all future work on Privacy related standards, that do not fall within the existing programs of work of the other 5 SCs, to SC 27. While Canada has and does support the work of developing Privacy Standards related to Privacy Protection being performed by SC 27, and is actively supports this work, Canada has and does maintain that it is inappropriate for SC 27 to be responsible for developing other Privacy related standards, for example Database Standards or Operating System standards. It is currently estimated that Privacy Protection standards equate to approximately <20% of the total standards needed for Privacy. It is also estimated that the work being currently performed by the other JTC 1 SCs represents a further 10% of the total needed. For the remaining 70% of standards work needed, that is not related to Privacy Protection, to be assigned to SC 27 has long seemed an anathema to Canada.

For the last 5 years Canada has been urging JTC 1 to establish an SC specifically to focus on Privacy Technology. Thus far, Canada has not met with success in this regard. The major impediment seems to be a lack of funding to support the secretariat for such an SC. While sufficient National Bodies express and interest and willingness to participate in such an SC, none are willing to fund the Secretariat.

Apart from the lack of Privacy Technology SC within JTC 1 to coordinate the activities of the six JTC 1 SCs and ensure that the products work together, and to develop privacy related technology standards, two other major impediments exist that are hampering the work. The first and most important is the lack of an internationally agreed set of harmonized privacy principles. While this is not a problem from a strictly Canadian perspective, it is for JTC 1. JTC 1 can not develop national specific standards. Thus without an agreed set of harmonized privacy principles it is very hard to develop standards that will respect all nations different sets of privacy principles The development of such a set can not be done by JTC 1, this is outside their purview, although they could perhaps find a way to publish such a set from another source.

The second major impediment is the disconnect between the Privacy Community, the privacy advocates and privacy management and policy people, and the technical standards community. It

Outre l'absence d'un sous-comité au sein du JTC 1 chargé de coordonner les activités des six SC du JCT 1, d'assurer la compatibilité des produits et d'élaborer des normes sur les technologies de protection de la vie privée, force est de relever deux autres grands inconvénients qui font obstacle aux travaux. Le premier et le plus important réside dans l'absence d'une convention internationale relative à un ensemble de principes harmonisés touchant la protection des renseignements personnels. Cela ne constitue pas un problème à proprement parler si l'on s'en tient rigoureusement à la perspective canadienne, mais c'est manifestement un problème pour le JTC 1. Comme ce dernier ne peut élaborer des normes nationales spécifiques, et en l'absence d'un ensemble convenu de principes harmonisés, il est extrêmement difficile de produire des normes conformes à tous les ensembles de principes que les différents pays se donnent à l'égard de la protection de la vie privée. Il n'appartient pas au JTC 1 d'élaborer un tel ensemble de normes, mais il pourrait cependant peut-être trouver un moyen de publier un tel ensemble, même s'il provient d'une autre source.

Le deuxième grand inconvénient réside dans le manque de concertation entre le milieu de la protection de la vie privée, les défenseurs, les dirigeants et les décideurs en la matière, et le milieu des normes techniques. Ce dernier ne s'attend pas à ce que le milieu de la protection de la vie privée rédige les normes techniques correspondantes, mais il a désespérément besoin de sa contribution à cet effet. Les lois et les politiques sont essentiellement de nature réactive et s'occupent de ce qui doit se passer une fois que la confidentialité de la vie privée est compromise. En revanche, les normes techniques sont essentiellement proactives et déterminent à l'avance comment la technologie et les communications peuvent fonctionner afin que la vie privée demeure protégée.

S'il est vrai qu'il reste encore beaucoup de choses à faire à ce chapitre, la plupart d'entre elles seront de peu d'aloi si ces trois inconvénients ne sont pas réglés. Pour peu qu'elle soit modeste, la moindre démarche en vue de supprimer ces inconvénients donnerait un sérieux élan à la société et supposerait un véritable progrès. Le JTC 1 n'est pas le seul à devoir faire du chemin, mais il est de ceux qui figurent en tête et ses normes sont essentielles si nous ne voulons pas nous retrouver avec des approches disparates

is not that anybody is expecting the Privacy Community to write the technical standards, but the technical standards community desperately needs the input of the Privacy Community. Legislation and Policy is primarily reactive, it addresses what is to happen when privacy is lost, technical standards are primarily proactive, they address how the technology and communications are to work in order that privacy will not be lost.

While there are many other things that need to be done, most of them will have little impact if these three impedimenta are not addressed. Finding a way forward on each of these would provide a significant boost to society and a significant step forward. JTC 1 is not the only place that things need to be done, but it is one of the most important. If we are not to end up with disparate approaches that will not work together JTC 1 standards are essential. A lack of standards in a specific domain can be compensated for by the generalized standards of JTC 1.

In Summary, there is a lack of coordinated leadership for Privacy within ISO/IEC JTC 1 and the Canadian JTC 1 group CAC-JTC1 needs to help of the Privacy Community in order to take a leadership position to correct this situation, and in developing privacy related technical standards.

incompatibles. Le manque de normes dans un domaine spécifique peut être compensé par les normes plus générales du JTC 1.

En somme, on constate un manque de leadership et de coordination à l'égard des normes de protection de la vie privée au sein de l'ISO/CEI JTC 1. Le groupe canadien CCC-JTC1 entend pour sa part aider le milieu de la protection de la vie privée et adopter une position de chef de file en vue de redresser la situation et d'élaborer les normes techniques qui s'imposent.

Annexe A

Normes de protection de la vie privée - Activités de l'ISO/CEI JTC 1/SC 17

Le sous-comité 17 de l'ISO/CEI JTC 1 élabore des normes dans le domaine de l'identification des cartes et des personnes. Il s'occupe de la protection de la vie privée dans le contexte des applications techniques des cartes et partant, de la sécurité des données générées par les cartes à puce et optiques et par toute la gamme des systèmes connexes, du moment de la saisie jusqu'à la destruction finale des données.

Le SC 17 n'examine pas actuellement les normes publiées sur la protection de la vie privée. Le président a toutefois rédigé deux procédures d'évaluation de l'impact sur la vie privée des technologies de pointe dans le domaine des cartes, en partenariat avec le Commissaire à l'information et à la protection de la vie privée de l'Ontario, et il est en train de mettre au point une troisième procédure relative aux applications des cartes sans contact.

Annex A

Privacy Related Standards Activities of ISO/ IEC JTC 1/SC 17

ISO/IEC JTC 1/SC 17 develops standards in the area of Cards and Personal Identification. SC 17 is concerned with privacy related to card technology applications. This includes data on smart and optical cards and throughout the entire related system, starting with the original capture of the data through to its final secure destruction.

SC17 is not currently reviewing published privacy standards, however the chairman has authored two Privacy Impact Assessment procedures for advanced card technologies in partnership with the Information & Privacy Commissioner Ontario and is in the final stages of a third, designed for contactless card applications.

Annexe B

Normes de protection de la vie privée — Activités de l'ISO/CEI JTC 1/SC 27

Le SC 27 de l'ISO/CEI JTC 1 élabore des normes dans le domaine de la sécurité (Techniques de sécurité des technologies de l'information). En vertu d'une décision adoptée au niveau du JTCI en 2004 (Berlin), le SC 27 s'est fait confier la responsabilité de passer au stade enquête dans les domaines de la protection de la vie privée et de la gestion des identités, qui semblaient exiger tous deux une certaine attention, tout en prévoyant des sauvegardes et/ou une protection; d'où la responsabilité du SC 27. Les rapports découlant du stade enquête devaient être déposés au JTC 1 en novembre 2006 à l'occasion de la réunion à Kruger Park (Afrique du Sud) en vue de trancher sur les recommandations et procéder à l'attribution des tâches correspondantes à un ou à plusieurs sous-comités au besoin.

En novembre 2005 (KL), deux groupes d'études (protection de la vie privée et gestion des identités) relevant du SC 27 ont présenté des rapports favorables aux dirigeants du SC 27 en recommandant que ce dernier adopte et institue des normes dans ces deux domaines. Ces recommandations ont été retenues et des appels ont été lancés pour la création d'un nouveau groupe de travail et la définition des nouvelles questions intéressant le SC 27. Cela s'est déroulé sans l'approbation officielle du JTC 1, malgré un certain laisser-faire ou feu vert officieux de la part de ce dernier (à en croire la direction du SC 27). On a fait valoir dans ce contexte que le SC 27 avait démontré sa fiabilité pour ce qui est de respecter les échéances de livraison des produits au marché, tout en rappelant que la protection de la vie privée et des renseignements personnels était un thème étroitement lié à son champ d'activité, la sécurité.

En réponse à l'appel à la création d'un groupe de travail à la suite de la réunion de KL, le Canada s'est fortement opposé à la création du GT 5 et des nouvelles questions connexes en recommandant plutôt la création d'un SC qui se pencherait exclusivement sur la protection de la vie privée, domaine qui pourrait éventuellement englober la gestion des identités.

Annex B

Privacy Related Standards Activities of ISO/ IEC JTC 1/SC 27

ISO/IEC JTC 1/SC 27 develops standards in the area of Security. By virtue of a decision at the JTCI level in 2004 (Berlin), SC27 has been attributed the responsibility of establishing study periods in the field of "Privacy" and "Identity Management", as these fields were considered as needing, as well as, providing safeguards and/or protection; hence the responsibility of SC27. The reports of the study periods were to be presented to JTC1 in Nov 2006 at the Kruger Park, SA meeting for recommendations and attribution to 1 or more SCs, if so deemed.

In November 2005 (KL), 2 study groups (Privacy and Identity Management) within SC27 presented favorable reports to SC27 management and the recommendations were for SC27 to adopt and establish standards for Privacy and Identity Management. These recommendations were adopted and calls for the creation of a new WG and for NWIs was made within SC27. This was without the official endorsement of JTC1, though it seemed officious on their behalf (as per SC27 management). It was explained that SC27 had a reputation for delivering product to the marketplace in a timely fashion and security was closely related to privacy and identity management.

In response to the call for the creation of a WG following KL, Canada strongly objected to the creation of WG5 and associated NWIs and recommended the creation of SC on Privacy, probably including Identity Management.

The title and scope for the new WG are "Identity management and privacy technologies", and the scope of SC27/WG 5 covers the development and maintenance of standards and guidelines addressing security aspects of identity management, biometrics and the protection of personal data.

Three current SC 27 projects from other WGs are transfered to WG5:

- Framework for Identity Management (ISO/IEC 24760)
- Biometric template protection (ISO/IEC

Baptisé « Gestion d'identité et technologies de domaine privé », le nouveau groupe de travail SC 27/GT 5 s'est vu confier l'élaboration et le maintien des normes et directives régissant les aspects touchant la sécurité de la gestion des identités, la biométrie et la protection des renseignements personnels.

Trois projets de normes en cours au sein du SC 27 ont ainsi été transférés d'autres groupes de travail au GT 5 :

- Cadre de gestion de l'identité* (ISO/CEI 24760)
- Protection du modèle biométrique* (ISO/CEI 24745)
- Contexte de l'authentification en biométrie* (ISO/CEI 24761)

Voici quelques-uns des autres sujets proposés comme nouvelles questions à envisager dans le domaine de la protection de la vie privée :

- Un cadre de protection de la vie privée
- Une architecture modèle pour la protection de la vie privée
- Des infrastructures pour la protection de la vie privée
- L'anonymat et les justificatifs d'identité
- Les technologies servant à renforcer la protection de la vie privée (PET)
- Les techniques de protection de la vie privée

D'autres sujets ont également été proposés dans le domaine de la gestion des identités et de la biométrie (les détails sont disponibles sur demande).

En l'absence d'une structure fondamentale globale sur la vie privée au sein de l'ISO, certaines réponses aux nouvelles questions sur la protection des renseignements personnels s'étendent au-delà du domaine des techniques de sécurité, dont pour le moment et plus précisément, le cadre de protection et l'architecture modèle pour la protection de la vie privée. Parmi les exemples de propositions reçues dans ce contexte, il serait question de formuler des prescriptions mondiales à l'égard des « informations personnellement identifiables » et d'énoncer un ensemble de « terminologies communes sur la protection de la vie privée » pour toute information et système de communication dans tous les pays et à tous les paliers d'administration. Il importe peut être de

24745)
- Authentication context for biometrics (ISO/IEC 24761)

Other topics requested as NWIs in the area of privacy include:

- A Privacy Framework
- A Privacy Reference Architecture
- Privacy infrastructures
- Anonymity and credentials
- Specific Privacy Enhancing Technologies (PETs)
- Privacy Engineering

Request for other NWI in identity Management and Biometrics were also made (details available on request).

Because no overall foundation on privacy exists within ISO, some responses to the privacy NWIs expand beyond the scope of security techniques, specifically to date, Privacy Framework, and Privacy Reference Architecture. Example of these proposals include determining globally the requirements for "Personally Identifiable Information" and a set of "common privacy terminologies" for any information and communication systems and in any jurisdiction. It may be important to note that many responses to these privacy NWI are presented by consortia that have related patented technologies.

Canada officially requested to SC27 that an SC on Privacy be created to address issues and requirements outside the scope of SC27, such as the ones described above, so that SC27 deal only with relevant and pertinent subjects related to information security techniques. The above NWIs have specifications beyond the scope and competency of SC27.

A NWI proposal for Authentication Assurance is currently submitted for review. It seeks to define what are the acceptable criteria and levels to authenticate an "entity and establish an "authentication assurance" or "Quality of Authentication (QoA) scheme; and it also seeks to enhance trust and confidence in authentication. It references E-Authentication documentation used by the Government of the USA. There is also a strong willingness for this NWI to establish metrics in order to quantify risk for identity management, but does not establish or define "identity" itself, which is beyond the scope of SC27, but not under

rappeler que de nombreuses réponses à ces nouvelles questions sur la protection de la vie privée sont présentées par des consortiums détenant des brevets sur les technologies connexes.

Le Canada a officiellement demandé au SC 27 la création d'un sous-comité spécial sur la protection de la vie privée, qui se pencherait sur les enjeux et les besoins qui ne relèvent pas du champ d'application du SC 27, tel que ceux décrits ci-dessus, de sorte que le SC 27 puisse se consacrer exclusivement aux sujets directement reliés aux techniques de sécurité de l'information. Les nouvelles questions ici décrites présentent des spécifications qui vont au-delà de la portée et de la compétence du SC 27.

Une proposition relative à la nouvelle question de l'authentification assurée est à l'étude. Elle cherche à définir quels sont les critères et les niveaux acceptables pour authentifier une « entité et établir un régime d'« authentification assurée » ou garantir la « qualité de l'authentification », tout en cherchant à accroître son degré de fiabilité. La proposition effectue des renvois à la documentation utilisée par le gouvernement des États-Unis en ce qui a trait à l'authentification électronique. On dénote également une volonté manifeste pour que des paramètres soient établis dans le cadre de cette nouvelle question en vue de quantifier les risques afférents à la gestion des identités, sans toutefois établir ou définir l'« identité » proprement dite, ce qui s'inscrit au-delà du mandat du SC 27, et ne correspond au mandat d'aucun SC de l'ISO en particulier.

Au niveau du JTC 1, le Canada a proposé la tenue d'un atelier sur la protection de la vie privée, où il s'agirait d'énumérer et de définir les responsabilités et la portée des divers travaux et projets de normes liés aux nouvelles questions, de sorte que l'on soit en mesure de justifier, documentation à l'appui, la nécessité d'instituer un sous-comité consacré au thème de la protection de la vie privée, tout en faisant la liaison entre la portée de ce SC et celle d'autres groupes pertinents.

the purview of one ISO SC in particular.

At the JTC1 level, Canada has proposed a Workshop on privacy to list and establish responsibilities and scope for the various standards, projects and NWI so that proof can be brought forward to demonstrate the need to have one SC on privacy with liaisons to pertinently scoped SCs and groups.

Annexe C

Normes de protection de la vie privée — Activités de l'ISO/CEI JTC 1/SC 31

Le SC 31 de l'ISO/CEI JTC 1 élabore des normes dans le domaine des techniques d'identification et de captage automatique des données, s'occupant notamment de l'identification par radiofréquence. Les activités de normalisation de l'ISO dans le domaine de l'identification par radiofréquence (RFID) pour la gestion d'objets sont axées sur la technologie, la conformité de la technologie, le contenu des données, la communication des données et la mise en œuvre. En ce moment et à en croire les membres du comité, aucune des technologies n'utilise des techniques d'encodage des données sur l'interface hertzienne. La fonction « Kill bit » a récemment été rajoutée à la norme ISO/CEI 18000-6 pour l'interface hertzienne. Les blocs de mémoire comprennent une protection par mot de passe.

Voir le tableau à la page suivante

Annex C

Privacy Related Standards Activities of ISO/ IEC JTC 1/SC 31

ISO/IEC JTC 1/SC 31 develops standards in the area of RFID. ISO Standards activities for RFID for item management are focused on technology, compliance of technology, data content, data communication and implementation. Currently – none of the technologies – according to committee members use data encryption techniques over the air interface. The Kill bit function was recently added to the ISO/IEC 18000-6 standard for the air interface. Memory blocks include password protection.

See table on page 75

Annexe C (suite)

Norme	Statut	Titre	Fonctions relatives à la protection de la vie privée
15961	IS/TR	Technologies de l'information – Identification par radiofréquence (RFID) pour la gestion d'objets – Protocole de données – Partie 1 : interface d'application (Révision de ISO/CEI 15961:2004)	Non comprises
24791-1	WD	Identification par radiofréquence (RFID) pour la gestion d'objets – infrastructure du système logiciel – partie 1 : Architecture*	À l'étude
24791-2	WD	Identification par radiofréquence (RFID) pour la gestion d'objets – infrastructure du système logiciel – partie 2 : Gestion des données*	Pas disponible
24791-3	WD	Identification par radiofréquence (RFID) pour la gestion d'objets – infrastructure du système logiciel – partie 3 : Gestion des applications*	Pas disponible
24791-4	WD	Identification par radiofréquence (RFID) pour la gestion d'objets – infrastructure du système logiciel – partie 4 : Interface des applications*	Pas disponible
24791-5	WD	Identification par radiofréquence (RFID) pour la gestion d'objets – infrastructure du système logiciel – partie 5 : Interface des dispositifs*	Pas disponible
24791-6	WD	Identification par radiofréquence (RFID) pour la gestion d'objets – infrastructure du système logiciel – partie 6 : Sécurité*	Pas disponible
24730-1	IS/TR	Techniques d'identification automatique et de capture de données – Systèmes de localisation en temps réel (RTLS)– partie 1 : Interface de programmation des applications (API)*	À l'étude
24730-4	NWIP	Techniques d'identification automatique et de capture de données – Systèmes de localisation en temps réel (RTLS)– partie 4 : Système de localisation mondial (GLS)*	À l'étude

Annex C (continued)

Standard	Status	Title	Privacy Functions
15961	IS/TR	Radio frequency identification (RFID) for item management -- Data protocol -- Part 1: Application interface (Revision of ISO/ IEC 15961:2004)	Not included
24791-1	WD	Radio Frequency Identification (RFID) for item management - Software system infrastructure - Part 1: Architecture"	Under Review
24791-2	WD	Radio Frequency Identification (RFID) for item management - Software system infrastructure - Part 2: Data Management"	Not Available
24791-3	WD	Radio Frequency Identification (RFID) for item management - Software system infrastructure - Part 3: Application Management"	Not Available
24791-4	WD	Radio Frequency Identification (RFID) for item management - Software system infrastructure - Part 4: Application interface"	Not Available
24791-5	WD	Radio Frequency Identification (RFID) for item management - Software system infrastructure - Part 5: Device Interface	Not Available
24791-6	WD	Radio Frequency Identification (RFID) for item management - Software system infrastructure - Part 6: Security"	Not Available
24730-1	IS/TR	Automatic identification and data capture techniques -- Real Time Locating Systems (RTLS) -- Part 1: Application programming interface (API)"	Under Review
24730-4	NWIP	Automatic identification and data capture techniques – Real Time Locating Systems (RTLS) – Part 4: Global Locating Systems (GLS)”	Under Review

Annexe D

Normes de protection de la vie privée — Activités de l'ISO/CEI JTC 1/SC 32

Le SC 32 de l'ISO/CEI JTC 1 élabore des normes dans le domaine de la gestion et de l'échange des données. Son mandat consiste à élaborer des normes axées sur les TIC dans ces domaines (y compris en commerce électronique). En l'occurrence, le SC 32/GT1 « e-commerce » (commerce électronique) joue un rôle de tout premier plan. Cela s'explique du fait que le commerce électronique se rapporte à tout échange de données électroniques numériques (EDI) qui comprend toute forme d'engagement entre des personnes (physiques ou morales). Cela comprend la reconnaissance de l'« individu » comme un sous-type particulier de personnes ayant des droits que les normes régissant le commerce électronique devraient être en mesure de respecter. Par ailleurs, dès le départ, les prescriptions juridiques et réglementaires qui s'appliquent à tout engagement conclu entre les parties intéressées et qui exercent une forme de « contrainte externe » font partie du modèle de référence EDI ouvert (ISO/CEI 14662) et sont décrites et documentées dans la norme ISO/CEI 15944 ainsi que dans le modèle d'opérations commerciales (BTM) correspondant.

Du point de vue du CCC JTC 1/SC 32, la grande majorité des prescriptions juridiques (et réglementaires) s'appliquant à la vie privée sont de nature à s'inscrire dans le domaine de la gestion et de l'échange de données. Le SC 32 a recensé les liens suivants entre ses activités et la protection de la vie privée :

1. GT 1 – Les normes relatives au commerce électronique revêtent une importance critique pour ce qui est de renforcer les prescriptions relatives à la vie privée.
2. GT 2 – Les normes relatives aux « métadonnées » n'appuient pas comme telles les prescriptions relatives au domaine privé, mais constituent plutôt des attributs du modèle de métadonnées et d'éléments de données contenant des concepts qui pourraient s'avérer utiles pour la gestion et l'échange de données personnelles.
3. GT 3 – Les normes relatives aux « Langages base de données » se concentrent sur le langage d'interrogation base de données (Standard Query Language) (SQL). Elles

Annex D

Privacy Related Standards Activities of ISO/ IEC JTC 1/SC 32

ISO/IEC JTC 1/SC 32 develops standards in the area of Data Management and Interchange. The mandate of ISO/IEC JTC1/SC32 is to develop ICT-based standards in the field data management and interchange (including e-commerce). Here, SC32/WG1 "e-Business" has a prominent role. This is because e-Business pertains to any electronic digital interchange (EDI) which involves the makes of any kind of commitment among Persons (natural or legal). This includes recognition of "individual" as a particular sub-type of Person having rights which e-Business standards must be able to support. Further, from the outset, legal and regulatory requirements which apply to the making of commitments among participating parties, i.e. as a type of "external constraint" form part of the Open-edi Reference Model (ISO/IEC 14662) and are addressed and supported in the ISO/IEC 15944 in its Business transaction Model (BTM).

From a CAC JTC1/SC32 perspective, the vast majority of the legal (and regulatory) requirements of "privacy" are of a data management and interchange nature. SC 32 has identified the following relationships between its activities and Privacy:

1. WG1 "e-Business" standards are of definite importance in supporting privacy requirements.
2. WG2 "Metadata" standards do not as such support privacy requirements but is metadata model and data element attributes likely do contain constructs which may be useful with respect to the management and interchange of "personal information"
3. WG3 "Database Languages" standards focus on Standard Query Language (SQL) standards do contain a number of features which support some of the privacy requirements.
4. WG4 "SQL Multimedia and Application Packages"" standards work on ISO/IEC 13249-6 re:"Data Mining" and ISO/IEC 13249-7 re: "History" may contain features.

It is noted that, in the development of the multipart ISO/IEC 15944 "e-business" standard, the need to be able to support legal requirements of a privacy/data protection nature has already been fully incorporated (along with public policy requirements of a similar nature pertaining to an

présentent certaines caractéristiques à l'appui des prescriptions relatives au domaine privé.

4. GT 4 – Les travaux de normalisation des « SQL/Multimédia et paquetages d'applications » s'inspirent de la norme ISO/CEI 13249-6 (« Exploration de données »). Le projet de norme ISO/CEI 13249-7 (« Historique ») pourrait contenir des caractéristiques s'y rapportant.

Rappelons que la nécessité de demeurer conforme aux prescriptions juridiques touchant la protection de vie privée et des renseignements personnels a été entièrement intégré aux diverses parties de la norme ISO/CEI 15944 « e-commerce » (Techniques descriptives sémantiques des accords d'affaires)(à l'instar des exigences du même ordre relevant de la politique publique touchant l'« individu » - en tant que droit humain -, dont la protection des consommateurs, l'accessibilité individuelle, etc.). Et c'est que l'intégration de ces exigences de la politique publique doit obligatoirement être prévue dans les normes relatives à la gestion et à l'échange de données qui favorisent la prise et l'échange d'« engagements » parmi les personnes dans leur rôle en tant que particuliers, organismes et/ou administrations publiques.

En somme, une fois que les besoins de protection de la vie privée seront identifiés, le CCC JTC 1/ SC 32 sera en mesure de déterminer (1) lesquels s'inscrivent dans le domaine de la « gestion et de l'échange des données »; (2) parmi ces derniers, si les normes existantes ou les projets de normes en la matière ont déjà fait entrer en ligne de compte les besoins de protection de la vie privée afférents à la gestion et à l'échange des données; (3) dans la négative, déterminer s'il y a lieu de lancer un nouveau projet d'élaboration de normes à l'appui de ces besoins, qu'il s'agisse d'une norme entièrement nouvelle ou de la répartition des projets dans le cadre d'une norme contenant plusieurs parties.

Voici quelques-unes des activités concrètes du groupe de travail du SC 32 dans le domaine de la protection de la vie privée :

Groupe de travail 1 – EDI ouvert (commerce électronique)

ISO/CEI 15944-1:2002 Technologies de l'information – Vue opérationnelle des affaires – Partie 1: Aspects opérationnels de l'EDI

"individual" (as a human right) such as consumer protection, individual accessibility, etc). This is because such public policy requirements must be supported in data management and interchange standards which address and support the making and exchange of "commitments" among Persons in their role as individuals, organizations and/or public administrations.

In conclusion, once "privacy" requirements have been identified , CAC JTC1/SC32 will be able to determine (1) which of these are of a "data management and interchange" ; (2) of these, whether or not, its existing standards or standards development work already supports those privacy requirements which are of a "data management and interchange" nature; and, (3) if not , determine whether or not it should launch a new standards development project in support of these requirements, either a new standard or project division of an existing multipart standard.

Specific activities of SC 32 WG related to Privacy include:

Working Group 1 - "e-Business"

ISO/IEC 15944-1:2002 Information technology – Business operational view – Part 1: Operational aspects of Open-edi for implementation

ISO/IEC FDIS 15944-5:2006 Information technology — Business Operational View — Part 5: Identification and referencing of requirements of jurisdictional domains as sources of external constraints.

Based on a JTC1/SC32/WG1 resolution (31 October-4 November, 2006) for an analysis by Canada and UK as to the need for a project split in 15944 for a new Part n: Identification and referencing of Privacy Protection requirements as a source of external constraints (provisional title). This analysis is based on the assumption that 65% + of this work is already done, i.e. imbedded in existing SC32/WG1 standards, the remainder data management aspects cover another 10-20%, leaving 15-25% additional work to fill existing gaps from a data interchange perspective.

Working Group 2 – Metadata

ISO/IEC 11179 (multipart) – Information technology - Metadata registries (MDR)

ouvert pour application
ISO/CEI FDIS 15944-5:2006 Technologies de l'information - Vue opérationnelle des affaires - Partie 5: Identification et référencement des exigences des domaines juridictionnels en tant que sources de contraintes externes*.

Conformément à une résolution du JTC 1/SC 32/GT 1(réunion du 31 octobre au 4 novembre 2006) voulant que le Canada et le Royaume-Uni procèdent à un examen conjoint de la nécessité de répartir les projets de la norme 15944 de manière à créer une nouvelle Partie n : Identification et référencement des exigences des domaines juridictionnels en tant que sources de contraintes externes (titre provisoire). Cette analyse prend pour postulat de départ que 65 % + de ce travail est déjà fait, c.-à-d. fait déjà partie intégrante des normes existantes du SC 32/GT 1, et que les aspects restants touchant la gestion de données représentent un autre 10 à 20 % des travaux nécessaires, laissant de 15 à 25 % à des travaux supplémentaires en vue de combler les lacunes sur le plan de l'échange des données.

Groupe de travail 2 – Métadonnées

ISO/CEI 11179 (plusieurs parties) – Technologies de l'information – Registres de métadonnées (MDR)*
ISO/CEI CD/FCD 19763 (plusieurs parties) - Technologies de l'information – Cadre d'interopérabilité des modèles de métadonnées*
ISO/CEI CD/FCD 20944 (plusieurs parties) - Technologies de l'information – Interopérabilité et liaison des registres de métadonnées *(MDRIB)

Groupe de travail 3 – Langages bases de données

ISO/CEI 9075-2:2003 (2e édition) Technologies de l'information – Langages de bases de données -- SQL -- Partie 2: Fondations (SQL/Foundation)

JTC1/SC32 Stade enquête – Sécurité de l'information SQL.

ISO/IEC CD/FCD 19763 (multipart) - Information technology - Framework for metamodel interoperability
ISO/IEC CD/FCD 20944 (multipart) - Information technology - Metadata Registries Interoperability and Bindings (MDRIB)

Working Group 3 - Database Languages
ISO/IEC 9075-2:2003 (2nd edition) Information technology -- Database languages - SQL - Part 2: Foundation (SQL/Foundation)

JTC1/SC32 Study Period "Information SQL Security.

Annexe E

Normes de protection de la vie privée — Activités de l'ISO/CEI JTC 1/SC 36

Le SC 36 de l'ISO/CEI JTC 1 élabore des normes dans le domaine des technologies pour l'éducation, la formation et l'apprentissage. Le SC 36 cherche à assurer que ces normes en TIC soient structurées de manière conforme aux prescriptions juridiques des domaines juridictionnels dans lesquels elles devront être mises en œuvre et utilisées, surtout s'il s'agit de capter et de gérer des informations qui entrent en ligne de compte dans les processus décisionnels touchant des particuliers. Les exigences juridiques et réglementaires les plus répandues en ce qui a trait aux particuliers comprennent l'accessibilité, le droit à la vie privée et à la protection de celle-ci, la protection des consommateurs, les droits de la personne, etc.

À l'appui des exigences visant l'accessibilité individuelle, le JTC 1/SC 36 est en voie d'élaborer une norme en plusieurs parties ISO/CEI 24751 intitulée « Adaptabilité et accessibilité individualisées en e-apprentissage, en éducation et en formation ». Les trois premières parties qui sont sur le point d'atteindre le stade FDIS (projet final de norme) sont :

- ► Partie 1 : Cadre et modèle de référence
- ► Partie 2 : Besoins personnels en matière d'« accès pour tous » et préférences de prestation numérique
- ► Partie 3 : Description des ressources numériques relatives à l'« accès pour tous ».

Ces trois normes, ainsi que les parties futures, soutiennent les exigences de protection de la vie privée et des données personnelles dans la mesure où elles s'appliquent à ce contexte. Le Canada est entièrement en faveur de l'élaboration d'une norme à parties multiples sur l'accès universel (« accès pour tous »), il est prêt à fournir la version française de la partie 1 tout en veillant au développement d'équivalents des termes et définitions en anglais et en français pour les parties 2 et 3, et il a l'intention d'en faire autant pour les parties futures.

Étant donné que le JTC 1/SC 36 tient à assurer que ces normes soient structurées de manière conforme aux exigences juridiques dans les domaines juridictionnels dans lesquels elles

Annex E

Privacy Related Standards Activities of ISO/ IEC JTC 1/SC 36

ISO/IEC JTC 1/SC 36 develops ICT standards in the area of Learning, Education & Training. JTC1/ SC36 wishes to ensure that its ICT standards are be structured to be able to support the legal requirements of the jurisdictional domains in which they are to be implemented and used. This is particularly so where such standards are utilized to capture and manage recorded information used in decision-making about individuals. Common legal and regulatory requirements of this nature include those pertaining to individual accessibility, privacy, protection, consumer protection, human rights, etc.

Here in support of "individual accessibility" requirements JTC1/SC36 is developing a multipart ISO/IEC 24751 standard title "Individualized Adaptability and Accessibility in e-Learning, Education and Training / Adaptabilité et accessibilité en e-apprentissage, education et formation". The first three parts which are reaching the FDIS stage are:

- ► Part 1: Framework and reference Model
- ► Part 2: "Access for All" Personal needs and Preference for Digital Delivery
- ► Part 3: "Access for All" Digital resources.

These three standards, as well as future parts, support privacy/data protection requirements as they apply in this context. Canada fully supports the development of the multipart "Access for All" standard and has resourced the French version of Part 1 and ensuring the development of English/ French language equivalent terms and definitions for Parts 2 and 3, and will do so for future parts.

Because JTC1/SC36 wishes to ensure that its standards be structured to be able to support the legal requirements in the jurisdictional domains in which they are to be implemented and used, is also is investigating the legal requirements of its P-members with respect to the ability to be able to support privacy / data protection requirements.. This is because the application and use of the majority of JTC1/SC36 standards involve the role of an individual as "learner". The result is that any recorded information on or about an identifiable individual as a "learner" is subject to applicable privacy/data protection requirements.

devront être mises en œuvre et utilisées, le SC 36 est également en train d'effectuer des recherches sur les exigences juridiques de ses membres en ce qui a trait à la capacité de respecter les exigences relatives à la protection de la vie privée et des renseignements personnels. Il en est ainsi parce que l'application et l'utilisation de la majorité des normes du JTC 1/SC 36 attribue un rôle d'« apprenants » aux particuliers. Résultat : toute information enregistrée sur ou à propos d'un particulier identifiable en tant qu'« apprenant » est subordonnée aux prescriptions pertinentes sur la protection de la vie privée/des renseignements personnels.

Eu égard à l'importance de veiller à ce que les projets d'élaboration de normes appuient également les exigences de protection de la vie privée et des données personnelles, le cas échéant, le JTC 1/SC 36 a décidé lors de sa réunion plénière en septembre 2006 à Wuhan (Chine) d'établir un groupe spécial sur la protection de la vie privée en lui confiant une enquête sur les exigences de protection de la vie privée et des données personnelles dans le domaine de l'éducation, de l'apprentissage et de la formation, c'est-à-dire du e-apprentissage ou apprentissage en ligne (voir le document JTC 1/ SC 36 N1436 qui est à la disposition des participants à l'atelier sur la vie privée).

Au Canada, le Conseil consultatif canadien sur les normes en apprentissage en ligne (CCCNAL), dont les principaux intervenants sont les ministères de l'Éducation, est en train d'entreprendre l'enquête du JTC 1/SC 36 sur la protection de la vie privée et les données personnelles pour le compte du CCC JTC 1/SC 36. La première phase s'est primordialement concentrée sur l'obtention de réponses de l'Alberta, de la Colombie-Britannique, de l'Ontario et du Québec. Les résultats de cette première phase seront distribués aux participants lors de l'atelier du CCN sur la vie privée. La deuxième phase s'étend aux répondants de manière à inclure tous les membres du Conseil des ministres de l'Éducation du Canada (CMEC) ainsi qu'aux ministres fédéraux et provinciaux détenant des responsabilités dans les domaines de l'apprentissage et de la formation. Le tout est en train d'être coordonné par le biais du CCCNAL.

Given the importance of ensuring that its standards development projects also support privacy/data protection requirements, where applicable, JTC1/SC36 decided at its September, 2006, Wuhan, China Plenary Meeting to establish an "Ad-Hoc Group on Privacy" and mandate this Ad-Hoc to undertake a Survey on Privacy/Data Protection requirements for Education, Learning and training (LET), a.k.a. "e-Learning" (see document JTC1/SC36 N1436 which is being made available to the Privacy Workshop).

In Canada, the eLearning Standards Advisory Council of Canada (eLSACC), whose major stakeholders are the Ministries of Education is implementing this JTC1/SC36 Survey on privacy/ Data Protection on behalf of CAC JTC1/SC36. The 1st Phase focused on obtaining responses from Alberta, British Columbia, Ontario and Québec. The results of this 1st Phase will be made available to the SCC Privacy Workshop. The 2nd Phase widens to respondents to include all the members of the Council of ministries of Education of Canada (CMEC) as well as those federal and provincial ministries with responsibility in the areas of learning and training. This is being coordinated via eLSACC.

Annexe F

Normes de protection de la vie privée — Activités de l'ISO/CEI JTC 1/SC 37

Le SC 37 de l'ISO/CEI JTC 1 élabore des normes dans le domaine de la biométrie. Les activités liées à la protection de la vie privée se concentrent au sein du groupe de travail no 6. Voici quelques-unes des activités en cours :

Projet de norme 24714 : Rapports techniques sur les « Aspects sociétaux et interjuridictionnels de la mise en œuvre des technologies biométriques »*
Partie 1 : « Guide aux questions touchant l'accessibilité, la protection de la vie privée, la santé et la sécurité dans le cadre du déploiement de systèmes biométriques destinés à des applications commerciales »*

Stade : PDTR (rapport technique)
Ce rapport technique a pour objet de servir d'orientation à la conception de systèmes biométriques en ce qui a trait aux aspects suivants :

- normes sociétales et prescriptions juridiques liées à l'échange de données biométriques entre des administrations et des pays distincts, particulièrement au chapitre de la protection de la vie privée et des renseignements personnels;
- convivialité des systèmes biométriques qui servent à identifier le plus grand nombre de personnes possible dans le contexte de la santé et de la sécurité.

La section 4.2.2 de l'ébauche actuelle se penche sur des questions de protection de la vie privée dans le contexte des exigences juridictionnelles découlant de l'emplacement et de la nature des systèmes biométriques déployés. La biométrie est décrite en termes des risques qu'elle peut présenter pour la vie privée aussi bien que comme une technologie permettant d'accroître le respect de la vie privée. Au nombre des risques, on compte des formes évoluées d'identification (possiblement secrète), les possibilités de mise en correspondance des données, le suivi des activités, le glissement des fonctions d'applications et la possibilité de fausser une identité.

La section 4.2.3 propose un ensemble de principes pour le respect de la vie privée dans

Annex F

Privacy Related Standards Activities of ISO/ IEC JTC 1/SC 37

ISO/IEC JTC 1/SC 37 develops standards in the area of Biometrics. Privacy related activities are concentrated within Working Group 6. Current activities include:

Project 24714: Technical Reports on "Cross-Jurisdictional and Societal Aspects of Implementation of Biometric Technologies"
Part 1: "Guide to the Accessibility, Privacy and Health and Safety Issues in the deployment of Biometric Systems for Commercial Application"

Development stage: PDTR
The purpose of the TR is to offer guidance on the design and development of systems using biometrics with regards to

- societal norms and legal requirements in the use of biometric data between different jurisdictions, in particular as regards privacy and personal data protection,
- usability of biometrics by the widest population of individuals health and safety.

Section 4.2.2 of the current draft addresses privacy issues in the context of the jurisdictional requirements arising from the location and nature of biometric deployments. Biometrics are described in terms of both potential privacy risks as well as a potential privacy enhancing technology. The privacy risks associated with biometrics include enhanced forms of (possibly covert) identification, possibilities for data linking, activity tracking. application function creep, and the possibility of "spoofing" identities.

A set of privacy principles for biometric deployments are offered in Section 4.2.3. These principles are modeled after the OECD guidelines and included such areas as consent, data limitation, retention policies, and security practices.

The importance of privacy protection for the acceptance of biometric systems is described in Section 4.7.2. Biometric system adopters are encouraged to be as transparent as possible about the biometric systems, including reasons for use, personal data that

les déploiements biométriques. Ces principes s'inspirent des directives de l'OCDE en la matière et s'appliquent à des domaines tels le consentement, la restriction des données, les politiques de conservation et les pratiques en matière de sécurité.

L'importance de la protection de la vie privée pour l'acceptation des systèmes biométriques est décrite à la section 4.7.2. On y encourage ceux qui adoptent des systèmes biométriques à se montrer aussi transparents que possible à propos de ces systèmes, en leur recommandant notamment d'expliquer aux intéressés les motifs du recours à ces systèmes, les renseignements personnels qui y seront saisis, la manière dont ces données seront stockées et partagées, ainsi que les risques connexes.

Dans l'ensemble, les allusions à la protection de la vie privée dans l'ébauche actuelle se limitent à introduire les concepts et les enjeux. Les conseils concrets sont peu nombreux et les exemples de contextes de déploiement sont plutôt restreints. En avril 2006, le Canada a présenté des commentaires proposant des améliorations ponctuelles, dont des renvois plus pertinents aux documents des normes existantes et une terminologie plus soignée. Il proposait également des directives précises pour la protection de la vie privée qui s'inspiraient des travaux réalisés par le Commissaire à l'information et à la protection de la vie privée de l'Ontario, ainsi qu'une étude de la mesure dans laquelle les gens sont souvent prêts à compromettre la confidentialité de leurs renseignements personnels pour des raisons de commodité.

Partie 2: « Applications pratiques dans des contextes précis »*

Stade : WD (Préparation – projet de travail)
Ce rapport technique va au-delà des questions générales discutées dans la Partie 1 pour s'occuper de technologies biométriques spécifiques (p. ex., empreintes digitales, reconnaissance de l'iris, reconnaissance faciale) et de contextes de déploiement précis (p. ex., les lieux de travail).

Ce document en est encore à ses tous débuts

is collected, how it is stored and shared, and any associated risks.

In general, the discussions of privacy in the current draft is limited to the introduction of concepts and issues. Little specific guidance is offered and only limited deployment contexts are considered. Canada submitted comments in April 2006 suggesting specific enhancements including better references to existing standards documents and terminology, suggestions for specific privacy guidelines based on work done by the Ontario Privacy Commissioner, and a discussion of the trade-offs people are often willing to make between privacy and convenience.

Part 2: "Practical application to specific contexts"

Development Stage: WD
This TR goes beyond the general issues discussed in Part 1 to address specific biometric technologies (e.g., fingerprint, iris, face recognition) and specific deployment contexts (e.g., workplaces).

This document is still in a very early form with many parts containing section titles only. Privacy is not addressed in a specific section of the document, although it is mentioned in some places. For example, with fingerprint technologies, privacy risks can be reduced if the fingerprints (or their templates) are stored in a token belonging to the user (e.g., a smart card). Also, when discussing workplace deployments, privacy requirements and regulations are discussed, including Canada's PIPEDA laws. Again, some privacy principles are offered for workplace usage, including proportionality, use limitation, and necessity.

Canada has submitted two sets of comments related to this activity, and is continuing to work to develop and improve the document.

et de nombreuses parties ne contiennent que les titres des diverses sections pour le moment. Aucune section n'y est entièrement consacrée à la protection de la vie privée, mais il en est question ça et là. Par exemple, dans le cas des technologies dactyloscopiques, la vie privée se verrait moins compromise si les empreintes digitales (ou leurs gabarits) étaient stockées dans un objet appartenant à l'usager (p. ex. une carte à puce). Par ailleurs, lorsqu'il est question du déploiement de ces technologies dans les lieux de travail, les exigences et règlements visant la protection de la vie privée, y compris la LPRPDE du Canada, y sont mentionnés. On propose enfin quelques principes régissant l'usage de ces technologies dans les lieux de travail, dont le principe de la proportionnalité, de l'usage limité et de la nécessité.

Le Canada a présenté deux ensembles de commentaires en ce qui a trait à cette activité et poursuit ses travaux en vue de développer et de peaufiner le document.