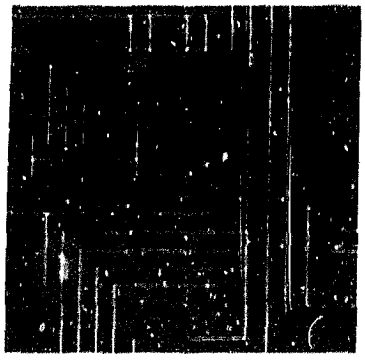
Government of Canada | Gouvernement du Canada



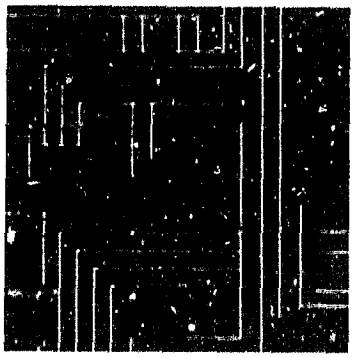
THE PROTECTION OF PERSONAL INFORMATION

BUILDING CANADA'S INFORMATION ECONOMY AND SOCIETY

Summary Report
of the Responses to the Discussion Paper

July 1998

Canada



THE PROTECTION OF PERSONAL INFORMATION

BUILDING CANADA'S INFORMATION ECONOMY AND SOCIETY

Summary Report
of the Responses to the Discussion Paper

July 1998

This publication is also available electronically on the World Wide Web at the following address:
http://strategis.ic.gc.ca/privacy

This publication is also available in alternative formats on request.
See distribution contact numbers listed below.

For additional copies of this publication, please contact:

Diane Breau
Electronic Commerce Task Force
Industry Canada
300 Slater Street, Room 2052C
Ottawa, ON K1A 0C8

Tel.: (613) 991-4029
Fax.: (613) 941-0178
Email: breau.diane@ic.gc.ca

Murray Long may be contacted at:

Murray Long Communications and Policy Consulting
640 LaVerendrye Dr.,
Gloucester, ON K1J 7C4

Tel.: (613) 747-9651
Fax.: (613) 747-6261
Email: murray.long@sympatico.ca

Cat. No. C2-355/1998
ISBN 0-662-63706-2
52007B

Aussi disponible en français sous le titre *La protection des renseignements personnels : Pour une économie et une société de l'information au Canada – Rapport sommaire des réponses au document de travail.*

Contents

Introduction

On January 27, 1998, Industry Canada and the Department of Justice released a consultation paper entitled *The Protection of Personal Information - Building Canada's Information Economy and Society*. A total of 83 submissions were received by the March 27, 1998 deadline for response, ranging from detailed submissions from industry associations to single page e-mails from private citizens. An additional seven submissions were received after the deadline. All seven late submissions are included in this analysis.

Of the 90 submissions, 22 were from individuals; included in this category were three from academics, four from privacy experts or consultants, and one from a member of the Alberta Legislature.

Among organizations, the federal Privacy Commissioner and the privacy commissioners for Alberta, British Columbia, Ontario and Quebec all responded. There were 10 submissions from consumer groups, one submission from a labour organization (the Canadian Union of Public Employees), four submissions from organizations within the health care sector, five submissions from organizations representing archivists, historians, librarians and records managers, and one submission from a law enforcement agency (the Royal Canadian Mounted Police). The Government of Alberta submitted a response, as did the European Union.

Among responses from business groups, there were five submissions from industry associations whose membership have an interest in information technology and electronic commerce issues. These were the Advanced Card Technology Association of Canada (ACT), the Canadian Association of Internet Providers (CAIP), the Canadian Advanced Technology Association (CATA), the Canadian Information Processing Society (CIPS), and the Information Technology Association of Canada (ITAC). There were seven submissions from business organizations representing both conventional retail and direct marketing interests. There was one submission from an organization representing media interests, the Canadian Newspaper Association. There were six submissions representing the positions of telecommunications companies subject to federal regulation through the Canadian Radio-television and Telecommunications Commission (CRTC), and three from the cable television industry, which is also subject to CRTC regulation. There were two submissions from organizations representing federally regulated financial institutions, and 14 additional submissions representing both federally and provincially regulated companies within the financial, insurance, securities, and credit reporting industries, as well as professional associations within this broadly defined sector.

In our analysis of submissions, we had to reflect on many thoughtful and original suggestions on how to construct, implement and enforce privacy legislation. On some points, there is a consensus of opinion. As might also be expected, some suggestions are diametrically contradicting. While these may represent both ends of the spectrum on a certain issue, in most cases, other suggestions present a degree of flexibility on how some issues might be addressed.

On some issues, there is as much divergence of opinion between sectors and within sectors as there is convergence. This applies equally to privacy commissioners, consumer groups, individuals and business organizations.

Moreover, within the business community, some submissions reflect the views of groups of professionals that work within an industry sector and, as such, the approach to issues is considerably different than the viewpoints of business organizations themselves. Business organizations may be subject to differing oversight regimes — federal, provincial, or both — or have no regulatory oversight.

Finally, there were a wide variety of models suggested as to how privacy protection could best be achieved within the commercial marketplace. As a result, it was a challenge to organize and compare the various responses in any meaningful way. The reader, however, benefits from knowing where particular views come from, and to what extent there are common opinions and views, or views that reflect a "business position," a "consumer position," or the position of privacy commissioners, for example.

To make the task of sorting out positions somewhat easier, categories of respondents have been organized as follows: Privacy Commissioners; Consumer Groups (including organized labour); the Health Care Sector; Law Enforcement; Government, including the European Union; Institutes; Archivists/Historical/Library Associations; the Telecommunications/Cable Sector; a broadly defined Financial Sector; Commercial/Retail Organizations; Information Technology Associations; and Individuals (including consultants, experts and academics). There may be some respondents to the Industry and Justice Canada discussion paper that feel this arbitrary grouping of interests does not fairly or accurately characterize their position within the overall community of interests. For this we apologize.

Some respondents provided insightful comments on their perceptions on the need for an information protection law, or detailed analysis on how their industry group currently protects personal information. We have chosen largely to omit these more general background comments in the summaries and focus instead on the specific responses to the 15 questions posed in the discussion paper. As a result, comments of some individual submissions are as long or almost as long as those of large organizations.

Readers seeking more detail and clarification of positions than exists in this analysis are urged to read the summaries. In addition, where even more specific detail is sought, readers can contact the Electronic Commerce Task Force for copies of selected submissions, many of which offer considerably more information on privacy issues and concerns, and private sector privacy initiatives than this document can possibly convey.

Murray Long

Suzanne Andrew

Executive Summary

There were 90 responses to Industry Canada and Justice Canada's discussion paper, *The Protection of Personal Information - Building Canada's Information Economy and Society*, ranging from detailed submissions from industry associations to single page e-mail notes. Among these submissions were two surveys, one by the Metropolitan Halifax Chamber of Commerce among its 1400 corporate members, the second conducted via the Internet by Privacy Forum Partners, a coalition of consumer groups, the Media Awareness Network and the Ottawa Public Library. The Chamber of Commerce survey elicited a range of opinion from support for simple legislation to strong opposition. Eighty percent of the 51 respondents indicated that legislation would have an impact on their business. The Privacy Forum Partners received 270 responses, all highly supportive of privacy legislation.

Submissions received from all parties responding to the Industry and Justice Canada discussion paper were summarized and analyzed in accordance with the 15 questions, although some comments were outside the scope of the discussion paper. Some submissions, both within the business community and among non-business groups, treated only a subset of the 15 questions and limited their comments to the issues of greatest interest to them.

To facilitate analysis, the submissions have been arbitrarily grouped into the following categories: Privacy Commissioners; Consumer Groups (including organized labour); the Healthcare Sector, Law Enforcement; Government including the European Union; Institutes; Archivists/Historical/Library Associations; the Telecommunications/Cable Sector; a broadly defined Financial Sector; Commercial/Retail Organizations; Information Technology Associations; and Individuals (including consultants, experts and academics).

Responses to a number of the questions indicated clear support for a particular direction. For example, the Canadian Standards Association *Model Code for the Protection of Personal Information* (CSA Standard) is almost unanimously regarded as the right place to start in drafting legislation, although privacy commissioners, consumer groups and some business organizations believe there is a need to add further obligations or make the legislation more precise than the existing CSA Standard.

There is also near-unanimous agreement on the need to harmonize federal and provincial privacy laws to ensure consistent application, prevent barriers to inter-provincial trade and discourage the growth of data havens. There is also strong agreement that the Uniform Law Conference of Canada (ULCC) represents the best overall forum to achieve harmonization of federal and provincial privacy legislation.

There is widespread support for the Office of the Privacy Commissioner of Canada to be

the oversight agency, and broad agreement that the Office of the Privacy Commissioner is the best body to educate the public about privacy matters.

Regarding sectoral codes, there is strong agreement that such codes play a useful role in protecting personal information, but there is little support for such codes replacing the law. There is also little support for start-up obligations such as registration of privacy codes with an accredited registrar or oversight body.

On several other questions there was a wide divergence of opinion. These included the question of disclosure without consent and exemptions to the legislation, as well as questions on enforcement powers, the creation of a tribunal or use of the Federal Court, the role of existing industry regulators and the requirement for privacy impact assessments.

On the issue of whether or not the CSA Standard is precise enough in setting out obligations, privacy commissioners, consumer groups, and individuals generally all believe changes are required to make the Standard more precise and add new obligations, such as a requirement to justify information collection purposes. Some business organizations also believe legislation would require more specificity to enable certain types of information-gathering and use, and to set clear and predictable rules under which businesses can operate.

Because the submissions from both consumer and business groups indicate a common concern about the need for precision, it would seem to make sense to revisit the CSA Standard in an attempt to accommodate these concerns. In their attempts to contribute to greater business certainty about information uses, some of the detailed suggestions provided in the submissions, however, may impinge on the flexibility of the current CSA Standard, an aspect of the CSA Standard that the majority of businesses assert should be maintained.

The majority business view is that the CSA Standard not be altered in any way, since it provides the flexibility necessary for business activities. Businesses noted that they require a light-handed legislative framework that does not unduly impede business activities. It may be possible to achieve the right balance by jointly examining issues of precision and obligations with the nature of the oversight powers proposed by different parties. In this case, the less precise the law is, the greater the oversight powers may need to be, and vice versa, to ensure that information privacy rights are adequately protected and an appropriate balancing of interests is maintained.

The issue of disclosure without consent and exemption to the legislation provides another opportunity to find a balance of interests that might accommodate the needs of all parties. Archivists and the media seek exemptions from the scope of the legislation for historical information and journalistic activities. Instead, including both activities as types of information that might be subject to use and disclosure without consent might accommodate these activities, while still ensuring other privacy protection principles, such as accountability, purpose definition and safeguards remain in place.

In the area of complaints investigation, there is general acceptance by all parties that consumers should deal directly with organizations first, and only when a complaint cannot be resolved should an oversight body become involved. There is clear support for the federal Privacy Commissioner having ultimate oversight responsibilities. There is very little support for federal sector regulators, such as the Canadian Radio-television and Telecommunications Commission (CRTC) or the Office of the Superintendent of Financial Institutions (OSFI), having ultimate oversight responsibilities. There is, however, some support for industry self-regulatory organizations to assist in the complaints resolution process.

In addressing enforcement powers, there is broad support, although not unanimous among business interests, for proactive oversight powers that would include investigation, independent of complaints. There is, however, a range of opinions on how compensation should be awarded. There are also mixed views on whether privacy assessments should be mandatory, and how they should be performed.

Highlights

The Highlights below draw from the Detailed Analysis section of this report where they are elaborated upon in greater detail. They represent the diversity of opinions expressed by respondents. In some cases, the authors have offered some suggestions to accommodate the interests of all parties.

(N.B. Conclusions are numbered and organized on the basis of the 15 questions within the consultation paper.)

1. It is generally agreed that the CSA Standard should be the basis for legislation. However, comments by various parties, including privacy commissioners, consumer groups, business organizations, special interest groups and individuals, on the need for greater precision and additional obligations should be considered in any drafting exercise.

2. Various business organizations and other parties suggested specific categories of information use that should be subject to disclosure without consent. Other parties, including privacy commissioners and consumer groups want an extremely limited and highly specific list of information use categories and situations where disclosure without consent would be allowed. It was also noted by some parties that no such list can be exhaustive. In light of these differing positions, the best approach may be to include a well delineated list of examples of disclosure without consent within the legislation, and guidance on circumstances under which such disclosures would normally be allowed. The suggestion made by a few parties that organizations be required to document and substantiate any such disclosures without consent is also worth consideration.

3. There is limited support for binding sectoral codes, and it is generally suggested by respondents that there be no provision within legislation to allow sectoral codes to replace legislation or have legal recognition, including interpretative value. One business submission, in particular, raised the issue of the interpretative value of such codes (i.e. courts, in determining penalties or awards would have to give due consideration to the manner in which the organization interpreted the legislation within its sectoral code). One consumer submission, however, suggested that a fundamental reason why greater precision is required within the legislation is to prevent organizations from using the "impenetrable defense" that they have applied subjective judgement to the CSA Standard in good faith. Perhaps, given these conflicting views, the question of interpretative value is best left to the courts without any direction within legislation.

4. The submissions indicate that the legislation should define "person" to include only natural persons to avoid giving organizations the information protection rights of individuals. The drafters of legislation should also consider whether to distinguish between widely available public domain information and public information that is not intended for widespread distribution or use. Where categories of data users seek exemptions from the legislation, the drafters should consider whether to exempt users from the full scope of the legislation or whether exemptions, if any, should be restricted to particular aspects (e.g. an exemption from the obligation to obtain consent before information collection, use or disclosure).

5. Support for registration procedures, where it existed, seems to be on the merits of creating a central repository of codes and contact individuals. Given the lack of support for this concept from privacy commissioners, and the availability of such information directly from organizations under the law, a registration process appears to be unnecessary.

6. Generally, all parties recognize the need for investigative powers when a complaint arises. Where detailed powers are recommended, they are generally in line with the existing powers of the federal Privacy Commissioner.

7. Consumer groups and privacy commissioners favour broad powers to address violations. Most parties support the power to publicize consumer complaints and non-compliance, without fear of liability, and several business and consumer groups as well as individuals suggest this is among the most important deterrent powers.

8. There is broad agreement that oversight bodies should have powers to conduct independent research *of a general nature*, since such research on new technologies and emerging privacy issues is of value to all parties. Most business submissions oppose proactive investigations, while privacy commissioners, consumer groups and individuals support broader powers to conduct investigations where multiple complaints, investigation and mandatory mediation suggest systematically inadequate information practices.

9. Most respondents agree that the federal Privacy Commissioner should be the oversight agency.

10. There is mixed support for the use of tribunals versus the Federal Court, and little in-depth discussion of the pros and cons of either approach. The majority of business groups prefer use of the Federal Court. Privacy commissioners and consumer groups are divided on the issue. Where a tribunal is preferred, it is generally on the basis of accessibility (e.g. the courts are clogged) and, in a few suggestions, to act as a national body that could play a role in harmonizing privacy protection across all jurisdictions (as in the Human Rights Tribunal or Competition Tribunal that were mentioned by a few parties as examples of such national bodies). Where a preference for the Federal Court exists, there is also mention in submissions from some consumer groups that the legislation should not prevent individual access to lower courts, such as provincial small claims courts, to claim damages and seek awards. In one consumer group submission, there is reference to a structured approach that would facilitate such legal actions.

11. There is clear support for the federal Privacy Commissioner having ultimate oversight responsibilities. There is very little support for federal sector regulators, such as the Canadian Radio-television and Telecommunications Commission (CRTC) or the Office of the Superintendent of Financial Institutions (OSFI), having ultimate oversight responsibilities. There is, however, some support for industry self-regulatory organizations to assist in the complaints resolution process.

12. Most respondents agree that public education should be the primary responsibility of the federal Privacy Commissioner. It should be listed as a duty under the proposed legislation, and adequate funds should be provided for it. Organizations should have an obligation to be open to the public about their own specific information use policies and practices, as specified within the CSA Standard.

13. There are differing views on the need for mandated privacy impact assessments. Business organizations are almost unanimously opposed to mandatory assessment which, in their view, might threaten technology innovation, create impossible hurdles for cash-strapped small companies and drive activities and jobs to other jurisdictions. Consumer groups have mixed views on mandatory assessments and who should perform them, and only one privacy commissioner supports legislated privacy assessments. It may be possible to accommodate the interests of all parties in protecting personal information while not unduly impacting the advance of new technologies and services by encouraging, rather than requiring, privacy impact assessments under legislation. Such assessments could be performed by accountable individuals within organizations and would be a consideration in any subsequent investigation by the federal Privacy Commissioner.

14. Most parties believe that harmonization is important, even critical, to the success of any legislated private sector privacy regime and to the marketplace, yet there are few specific instructions on how to accomplish harmonization. There are conflicting views on whether the federal government should move unilaterally on legislation ahead of the provinces.

15. There is strong support for the work of the Uniform Law Conference of Canada (ULCC), which is drafting a model privacy law, but other forums should also be used to advance harmonization of privacy protection across all jurisdictions. All forums should involve stakeholder input to the maximum extent.

Detailed Analysis of Submissions

This analysis of comments and recommendations made to Industry Canada from the various submissions follows the order of the questions from Part 3 (*Your Turn*) of the consultation paper. A range of specific detailed suggestions about implementing privacy legislation in the private sector has been captured, but should not be considered as exhaustive. For further detail, refer to the submissions.

Obligations

1. Is the CSA Standard the base from which to start in drafting legislation? Is it precise enough in setting out obligations or do some obligations require further elaboration? Are there any additional obligations not set out in the CSA Standard that should be included in the legislation?

Question 1 elicited the largest number of comments of any question. This reflects a wide divergence of opinion on private sector privacy legislation and how it should be approached.

All privacy commissioners, consumer groups, public institutes, academics, privacy experts, consultants and other individuals fully support legislation. The European Union and Alberta Government submissions also support moving forward with a federal private sector privacy law, although the Alberta Government strongly stresses the need for ongoing consultation with the provinces before any federal legislation is enacted.

In contrast, not all respondents within the private sector accept that legislation is necessary. For example, the Canadian Gas Association and Faneuil ISG Inc., a direct marketing firm, state that additional privacy protection is unwarranted at this time. Equifax Canada believes that privacy law should not proceed without empirical evidence that voluntary codes are inadequate. Credit Union Central of Canada also believes voluntary codes are preferable to law.

The majority of responses from the federally regulated telecommunications and cable industries also state a preference for privacy self-regulation. Within the federally regulated banking industry, the Canadian Banking Ombudsman is less supportive of private sector privacy law than is the Canadian Bankers Association. Among other industry submissions, the views on the need for a private sector privacy law range from clear support and acceptance to a preference for voluntary codes. Total responses reveal that, of 39 business organizations responding to the consultation paper, 17 favour legislation, 12 do not, and six organizations are ambivalent.

Regardless of their views on the need for legislation, virtually all respondents accept the CSA Standard as a good starting point. The CSA Standard is seen by almost all parties as a document that was developed by consensus, with input and broad support from industry, government, and consumer organizations.

Views differ widely, however, on whether the CSA Standard should be adopted as is, or whether it requires more precision.

Privacy commissioners, consumer groups, and most individuals favour greater precision. The federal Privacy Commissioner, in particular, offers specific and detailed wording changes to the CSA Standard. In contrast, the majority of business organizations would prefer to see the CSA Standard adopted without any changes. Their view, generally, is that the CSA Standard provides necessary flexibility for business and that more onerous requirements could stifle private sector activity.

Not all business organizations agree on this point, however. In response to *Question 1*, as well as *Questions 2 & 4*, which deal specifically with the content of the CSA Standard, a number of business organizations call for more precision where it would create "clear and predictable rules" and promote certainty in matters of interpretation, as well as meet the needs of their industry.

The comments made by those seeking greater precision cover a range of issues, although there is a strong focus among privacy commissioners, consumer groups and individuals on greater specificity in defining information collection purposes and ensuring that defined purposes are legitimate. Other key concerns are the use of implied consent, how consent should be obtained, and how data should be protected when it is processed either by third parties or outside of Canada. This question also elicited comments on several side issues that are related to personal information collection and use, such as surveillance, e-mail privacy, and the collection and use of biometric data.

The viewpoints on the use of the CSA Standard and other issues are described below by category. Please note that not all respondents answered all questions. In the responses to each question, comments appear only where specific organizations or individuals chose to make them.[1]

---

[1] There were a number of instances where the views of organizations or individuals on specific issues are ambiguous and no clearly defined position could be determined. In such cases, views are generally not represented. Also, in a small number of instances, organizations or individuals proposed a model for privacy regulation that did not correlate with some of the questions. Rather than attempt to fit the model to the question, some of these comments have been omitted here, but can be found in the individual submissions.

Privacy Commissioners

Responses were received from the Privacy Commissioner of Canada (federal Privacy Commissioner), the Information and Privacy Commissioner of Alberta, the Information and Privacy Commissioner for British Columbia, the Information and Privacy Commissioner of Ontario and the Commission d'accès à l'information du Québec (Commission d'accès).

All privacy commissioners support statutory privacy legislation, but all view the CSA Standard as requiring substantive improvements if it is to become the basis for a privacy law.

The federal Privacy Commissioner provided specific comments on each of the CSA Standard's 10 principles. This was the only submission suggesting precise wording changes to the CSA Standard. The main points appear below:

- Under *Accountability*, add a provision that organizations are legally responsible for information provided to third parties for use on their behalf.

- Under *Identifying Purposes*, add a provision that, before any personal information is collected, the purposes be both assessed and documented (and be lawful), and the individual be informed of purposes the obligatory or voluntary nature of their consent, the consequences of failing to consent, the recipients of the information and its uses.

- Under *Consent*, add a provision that consent be plainly and clearly explained, freely given, informed, specific and express concerning all types of information uses and potential recipients, and authorized for a limited period.

- Under *Limiting Collection*, add a provision that information collection be limited to that which is required by law or for the specific identified purposes, and be collected directly from the individual, except where health or safety is directly at risk or as required by law.

- Under *Limiting Use, Disclosure, and Retention*, add a provision that personal information be used or disclosed only for the specific purposes for which it was collected and with consent of the individual, except for health and safety or as required by law, and that such information not be disclosed without comparable safeguards, and that it be retained only as long as necessary for the purposes and securely destroyed thereafter. All personal information should be treated as confidential and released only to those who need to know, and with a confidentiality agreement for third parties. No other releases should take place without the knowledge or consent of the individual or as required by law.

- Under *Accuracy*, replace "used" with "used or disclosed."

- Under *Safeguards*, add a provision that organizations and their agents shall protect personal information by physical, organizational and technological safeguards against accidental or unauthorized access, modification or destruction.

- Under *Openness*, replace "unreasonable effort" with "unreasonable cost or effort" and add that organizations should make available specific information about their management of personal information and their complaints resolution policies and practices.

- Under *Individual Access*, replace the wording of the principle with: "Upon request, an individual shall be informed of the existence, use and disclosure of his or her personal information, and shall be given access to his or her information without cost or unreasonable effort, except as legally allowed. An individual shall be able to challenge the accuracy and completeness of the information and have it amended, updated or deleted as required by the circumstances. Access, correction, amendment and deletion requests shall be addressed within set time limits."

- Under *Challenging Compliance*, add a provision that organizations must respond to challenges within set time limits and that, if the individual remains dissatisfied with an organization's response, the individual shall have the right to appeal the response to the central oversight agency.

The Information and Privacy Commissioner of Alberta views implied consent as inconsistent with fair information practices and recommends that legislation specify consent in writing. The Commissioner adds that the law should require individuals to be advised when information is released to a third party without consent.

The Information and Privacy Commissioner for BC does not support the CSA Standard as a basis for legislation and calls upon the government to base legislation upon the far stronger information protection provisions of the *European Directive on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data* (EU Directive) and the *B.C. Freedom of Information and Protection of Privacy Act.*

The Information and Privacy Commissioner of Ontario recommends an opening section within the legislation to better define purposes, and greater clarification of acceptable purposes for information collection in order to narrow and solidify the *Limiting Collection* principle of the CSA Standard.

The Commission d'accès suggests Québec's *Bill 68, An Act Respecting the Protection of Personal Information in the Private Sector* (the Québec *Act*) is a better basis for legislation than the CSA Standard.

Consumer Groups (including organized labour)

A total of 11 submissions were received from consumer and public advocacy groups, including the Canadian Union of Public Employees (CUPE). However, the number of actual consumer and public interest groups represented by these submissions is considerably greater.

The British Columbia Public Interest Advocacy Centre submitted comments on behalf of nine other organizations in B.C., collectively known as BCOAPO (*see the Index for a listing of these groups*). The Fédération nationale des associations de consommateurs du Québec and Option Consommateurs (FNACQ/OC) filed a joint submission, and a group known as the Privacy Partners Forum (Privacy Partners) filed a submission which included results of an electronic survey conducted jointly by seven organizations.

All consumer organizations support a federal private sector privacy law, but none believe the CSA Standard is currently sufficient as a basis for legislation.

The B.C. Civil Liberties Association (BCCLA) believes the CSA Standard should incorporate a new principle of justification to limit information collection to legitimate reasons, with organizations required to justify purposes if challenged. BCCLA notes references to "a serious and legitimate reason" in Section 4 of the Québec *Act* and to "legitimate purposes" in Article 6 of the EU Directive as a precedent for a principle of justification. BCCLA adds that privacy legislation must also apply to the process of intruding on privacy, stating that practices of organizations such as mandatory drug-testing of employees impinge on privacy interests, even if no personal data is ultimately extracted.

The B.C. Freedom of Information and Privacy Association (FIPA) supports the principle of justification and adds that a right of privacy should ultimately be incorporated into the *Canadian Charter of Rights and Freedoms*. This view is shared by Canada's Coalition for Public Information (CPI), Privacy Partners, and the Public interest Advocacy Centre (PIAC).

CPI also believes legislation should incorporate both the CSA Standard and the fair information practices contained within the Industry Canada consultation paper.

The Consumers' Association of Canada (CAC) says negative option consent should not be allowed in the legislation, with any exceptions fully justified. The purpose for data gathering should be stated precisely and data mining should be prohibited. The CAC also suggests addition of the 12 principles of the New Zealand Health Information Privacy Code.

The Consumers' Association of Canada - Ontario (CAC Ontario) supports the CSA Standard as a basis for legislation, with no comment on additional obligations. The Consumers Council of Canada (CCC) also supports the CSA Standard, but adds that individuals should have sole rights of ownership to their personal information and rights to control use.

FNACQ/OC believes new private sector privacy law could be based on the CSA Standard, but also upon the ULCC draft and the Québec *Act*, which offers more detail on obligations.

Privacy Partners opposes vague or general statements of purposes and states that legislation must precisely define consent so the individual knows permission is being sought, and

is cognizant of how data will be collected and used. All uses should be based on an opt-in provision with consent in writing wherever practical. Purposes should be highly specific with no denial of services or other penalties for refusing consent to unnecessary information collection. There must be a clear limitation period for information use and specific consent should be required to share information with other affiliated or non-affiliated organizations or departments of a company. Special protection is required for genetic and health information, and parents and guardians should control use of children's information.

Privacy Partners adds that the consultation paper definitions of privacy and informational privacy should be incorporated into the legislation. Since employees may be the only people within organizations aware of information misuses, the legislation should also contain special protection for whistle blowers.

In addition, PIAC wants a privative clause in legislation denying parties the right to contract out of legislation. PIAC also suggests that two of the *Telecommunications Privacy Principles* be added to the legislation. These principles call for privacy considerations to be addressed specifically when new services are provided and, when a new service that compromises privacy is introduced, that appropriate measures be taken to maintain customers' privacy at no extra cost unless there are compelling reasons for not doing so.

PIAC also wants the definition of "organization" to be tightened in legislation to address information use by affiliates or the rights of individual data subjects in the event of a merger. PIAC adds that, unless the law has a substantive statutory limitation on information collection purposes, the consent requirement should provide more guidance on an organization's obligations to notify the individual about information uses, especially when implied consent is used. Legislation should also set a time limit after which destruction of personal information must proceed unless the company can prove continuing need. Once a customer relationship ends, data should be depersonalized or destroyed.

BCOAPO adds that greater specificity is required to prevent organizations from using the "impenetrable defence" that they have applied subjective judgement to the CSA Standard in good faith. BCOAPO proposes written consent as the norm, suggesting that, when implied consent is used, there should be an onus on organizations to show that consent was actually given. BCOAPO adds that lack of specificity in purposes should be a basis for invalidating consent to information collection, retention or transfer. BCOAPO calls mere documentation of purposes a "meaningless exercise."

CUPE believes federal legislation should encompass companies contracting with the federal government as well as federally regulated companies, and that contracting-out of information processing or situations where private corporations gain access to sensitive data should be governed by strict rules. CUPE adds that legislation must limit use of worker personal data only for purposes for which it was collected and only for reasons directly relevant to employment. All data should be secured with reasonable safeguards, with special protections for

medical data. Workers' personal data should not be communicated to third parties without express written consent except in emergency situations, as required by law, or as necessary for the conduct of the employment relationship. Workers should be regularly notified about the personal data held about them.

CUPE also notes specific concerns about health information, stating that legislation should affirm the principles of the *Canada Health Act* governing both public and private sectors, differentiate between health information for the public good and commercial interests, protect patient privacy and confidentiality of health data, ensure that personal health information is used only for its originally intended purpose, and exclude third parties such as insurance companies, employers and pharmaceutical companies from having direct access to health information.

Health Care Sector

IMS Canada (IMS) and the Canadian Dental Association (CDA) believe the CSA Standard is the right place to start, although CDA adds that the issue of self-determination of health records should be addressed. The Canadian Institute for Health Information (CIHI) recommends the legislation differentiate between person-identifiable, non-identifiable and anonymous data. CIHI would also like to see a differentiation between private non-profit and private for-profit uses. The Canadian Nurses Association (CNA) also wants the identifiable/non-identifiable issue to be addressed, with a differentiation between commercial and public interest uses. The CNA adds that the law must allow extended retention of specific information, especially if it can be rendered anonymous, and must also provide an avenue to seek the agreement of the data subject to use data for non-intended purposes.

Law Enforcement

The Royal Canadian Mounted Police (RCMP) recommends that legislation be strengthened to include certain security principles, including the application of safeguards throughout the information lifecycle, education on principles and safeguards for data owners and users, regular evaluation of safeguards including risk assessments, a requirement that non-traditional work or information storage environments (e.g. telework and data storage services) not diminish data security responsibilities, and the application of standards consistently across information management systems.

Government (including the European Union)

The Alberta Ministry of Science, Research and Information (Alberta) supports the CSA Standard as a basis for legislation, but adds that the unique privacy requirements of personal health information may require a separate legislative framework.

The Director General of DGXV (Internal Market and Financial Services) of the European Commission (EU) also supports private sector legislation in Canada based on the CSA Standard, recommending that a provision on data transfers outside of Canada be included in the law.

Institutes

The Fraser Institute would prefer to see privacy protection within the private sector dealt with through existing law rather than incorporating a whole new system of regulation. Violation of privacy should be prosecuted as theft, subject to immediate and heavy sanction. The courts should be relied upon to incorporate theft of privacy into the existing body of law.

The University of Ottawa Human Rights Research and Education Centre (the U of O Centre) wants the law to incorporate a number of recommendations from the proposed Charter of Privacy Rights from *Privacy: Where Do We Draw the Line?*, the Report of the House of Commons Standing Committee on Human Rights and the Status of Persons with Disabilities. These recommendations state that everyone is the rightful owner of their personal information; everyone is entitled to expect and enjoy anonymity unless the need to identify individuals is reasonably justified; and exceptions infringing on privacy rights should only be allowed if the interference is reasonable and can be demonstrably justified. In the Centre's view, the law should specify that information can only be collected for reasonable and demonstrably justified purposes. The Centre also suggests the legislation should contain the definitions of privacy and informational privacy specified in the Industry Canada and Justice Canada discussion paper.

Archivists/Historical/Library Associations

The Canadian Legislative and Regulatory Affairs Committee (CLARA) of the Association of Records Managers and Administrators (ARMA International) believes the "except where inappropriate" clause under Consent (*Principle 3*) of the CSA Standard gives too much discretion to information managers and is a potential area of dispute with consumers. CLARA also believes the requirement that information be retained only as long as necessary for the fulfillment of purposes (*Principle 5*) is overly vague since it does not clarify which purposes take precedence in determining an information retention period. Similarly, the phrase "required by law" may not adequately cover all situations. CLARA believes the requirements that individuals be informed of the existence, use and disclosure of personal information and be given access (*Principle 9*) are inappropriate as they go beyond the right of access embodied in the *Privacy Act* and equivalent provincial legislation, both of which establish specific exceptions to this right of access.

The Association des archivistes du Québec believes the law must allow society to maintain its "collective memory" by allowing the disclosure and use of personal information for research purposes, without consent, as allowed under the *Privacy Act* and the EU Directive — as long as this does not harm the individual involved. The legislation should also allow businesses to pass on personal information of historical value to any archive service without an individual's consent. The receiving organization should be obligated to destroy any personal information once it is no longer useful.

The Canadian Historical Association/Société historique du Canada (CHA/SHC) and the Institut d'histoire de l'Amérique française (Institut) believe legislation must recognize heritage issues, and are particularly concerned about building finality into data use, followed by

destruction. Both organizations state that legislation should not affect the ability of archives to collect, preserve and make available data collections to qualified researchers, nor should it limit the life of data necessary for historical research.

The Institut adds that legislation should set a time limit for the duration of information protection, specifically recognize personal data as also being archival material, and recognize the role of institutions and heritage organizations in maintaining this information.

The Ontario Library Association (OLA) wants legislation to be compliant with the *EU Directive*.

Telecommunications/Cable Sector

There were nine submissions from the federally regulated telecommunications and cable industries. These were: AT&T Canada Enterprises (AT&T); one collective submission by ACC TelEnterprises Inc., AT&T Canada Long Distance Services Company, Call Net Enterprises Inc., fONOROLA Inc., and Westel Telecommunications Ltd. (the AT&T Companies); the Cable Television Standards Foundation (CTSF); the Canadian Cable Television Association (CCTA); the Canadian Wireless Telecommunications Association (CWTA); Microcell Communications Inc. (Microcell); Rogers Communications Inc. (Rogers); Stentor Telecom Policy Inc. (Stentor) commenting on behalf of most Stentor and Mobility Canada companies; and TELUS.

Of these, only the CWTA and Microcell openly express support for legislation.

Nevertheless, all organizations state that the CSA Standard is the right starting point if legislation is to proceed, with all but one organization supporting the use of the Standard without further changes. Only Microcell suggests the wording of the CSA Standard needs to be more precise.

The AT&T Companies note, however, that the CRTC should receive direction from the Minister of Industry to delete the confidentiality of customer information provisions from the telecommunications carriers' Terms of Service, since they believe these provisions are inconsistent with the CSA Standard.

Stentor also adds that the legislation must provide for a transition period to allow companies to develop tailored codes and implement necessary practices to deal with both new and previously collected personal information.

Financial Sector

The financial sector contained submissions from both federally and provincially regulated organizations in banking, insurance services, securities regulators and stock exchanges, accountants, and organizations representing the interests of professionals who work within this broadly defined sector.

The Canadian Bankers Association (CBA) supports the proposed "light, flexible and effective" legislation based on the CSA Standard and says the Standard as it currently stands should be restated in the law in its entirety rather than being referenced. The Canadian Banking Ombudsman (CBO), however, does not support private sector privacy legislation, but believes the CSA model code should be recognized as a legislated standard for personal information protection, much as the generally accepted accounting principles (GAAP) are recognized as a compulsory industry standard with the effective weight of law.

Canada Trust and the Association of Canadian Financial Corporations (ACFC) support legislation based on the CSA Standard. ACFC states that sectoral codes are the most appropriate place to further detail obligations, while Canada Trust views further obligations as distorting the balance of interests. The Canadian Association of Financial Institutions in Insurance (CAFII) and the Canadian Life and Health Insurance Association (CLHIA) also support legislation based on the CSA Standard, without additional obligations. CAFII notes that the need for flexibility in obtaining consent must be recognized in the electronic age.

The Insurance Council of Canada (ICC) and Equifax Canada (Equifax) do not support legislation. ICC states that the property and casualty (P&C) industry does a good job with self-regulation. Equifax says there is no empirical evidence that voluntary codes have proven, or will prove, inadequate. Credit Union Central of Canada (Canadian Central) also prefers voluntary sectoral codes. However, all three organizations view the CSA Standard, as it now stands, as the right basis, if legislation is deemed necessary.

The Certified General Accountants Association of Ontario (CGA Ontario) supports legislation based on the CSA Standard, but adds that more detail is required. CGA Ontario suggests legislation should provide more specific guidance on consent for sensitive information and positive opt-out opportunities for non-essential information, along with more elaboration on when a subsequent use or disclosure of information would be consistent with original purposes and encompass original consent. CGA Ontario adds that the Access principle of the CSA Standard is vague on exemptions to the right of access, the time that may be taken, the fees that may be charged, and the circumstances when businesses may be required to provide personal information correction notices to third parties.

CGA Ontario also wants prohibitions on collecting and storing sensitive information such as political or religious opinions, trade union membership, race, health or sex life without legitimate need or appropriate safeguards, although collection of financial information required by business should not be so restricted. CGA further states that it should be an individual's decision whether personal information is used beyond the original purposes, and that new legislation should contain specific provisions on consent and the use of personal information for target marketing, data mining and other unrelated purposes.

Employees from Deloitte and Touche (Deloitte employees) also support CSA Standard-based legislation, but call for more specificity in the Safeguards and Openness principles. Under

Safeguards, broad references to technological measures should be augmented with a specific requirement to match the security level to the sensitivity of the information and to assess the viability of security measures on an ongoing basis. Deloitte employees also suggest organizations be required to match the methods of providing information about company privacy policies to the method of request, and that allowing organizations to mail responses to on-line requests directly conflicts with the purpose of setting out the Access principle in the face of emerging technologies.

A submission from Bennett Gold, Chartered Accountants does not deal with the substance of the Industry Canada discussion paper, but says that the CA WebTrust seal of assurance developed by the Canadian Institute of Chartered Accountants and the American Institute of Certified Public Accountants should be adopted by the government as the audit and assurance component for electronic commerce in Canada. Bennett Gold states that trained and licensed chartered accountants should also be given the franchise for audit and assurance of electronic commerce and information protection.

Commercial/Retail Organizations

The Canadian Direct marketing Association (CDMA), Westcoast Energy/Enlogix Inc. (Enlogix), and the Sudbury and District Chamber of Commerce support legislation based on the CSA Standard with no further precision or obligations. Enlogix notes, however, that organizations should be required to publish complaints-handling experiences in summary form and retain records of complaints for audit purposes.

The Canadian Gas Association (CGA) opposes legislation, adding that any proposed legislation must avoid conflict with competition laws and should not set specific time limits for data retention or limit information use purposes. CGA notes the gas industry's requirements to collect and use customer data over a 20-year planning horizon. CGA also wants any legislation reviewed on a periodic basis (at least every five years), similar to sections 88 and 89 of the Québec *Act*.

Dun & Bradstreet Canada (D&B) raises concerns that the wording of the CSA Standard does not set clear and predictable rules, and is too restrictive in some areas. D&B notes that the CSA Standard is stricter than the *EU Directive* in limiting use or disclosure of information. D&B warns that overly restrictive rules would prevent disclosures of information, such as bankruptcy proceedings, that is of justifiable interest to the business community.

The Canadian Newspaper Association (CNA) expresses concerns about the CSA Standard in the context of journalism, as the organization feels the Standard creates onerous obligations on editorial processes, sets up uncertainty as to its scope and application in terms of media compliance, and undermines editorial independence. The CNA says legislation should be consistent with the *Universal Declaration of Human Rights* that guarantees the media's freedom of expression and its ability to "seek, receive and impart information and ideas."

Information Technology Associations

The Advanced Card Technology Association of Canada believes the CSA Standard is logical and easy to understand, but it should be compared with the EU Directive and provincial privacy codes and the strongest standard used. The Canadian Advanced Technology Association (CATA), the Canadian Association of Internet Providers (CAIP) and the Information Technology Association of Canada (ITAC) all support the CSA Standard without further changes. CAIP notes, however, that the law must clarify which parties are accountable for privacy law violations, stating that Internet Service Providers (ISPs) should not be liable for personal information disclosure by their customers or for inadvertent information disclosure of personal information as a result of cooperating with law enforcement agencies.

The Canadian Information Processing Society (CIPS) believes the CSA Standard should provide more guidance on intrusive data mining and computer matching, does not go far enough in specifying record-keeping requirements when data is disclosed to third parties, is silent on transborder data flow, and may allow implied consent to veil intrusive practices by marketers that, although not deceitful, are not fully informed.

Individuals (including consultants, experts and academics)

This question elicited considerable comment from the 22 individuals who responded. All individuals, except one, support the CSA Standard as the best place to start. No individual thought the CSA Standard was sufficient without changes. Changes suggested include:

- adding a principle of justification of collection;
- adding two principles from the proposed Charter of Privacy Rights from *Privacy: Where Do We Draw the Line?*, citing a duty to limit information collection to what is necessary and justifiable under the circumstances, and a duty not to disadvantage people because they elect to exercise their privacy rights;
- incorporating principles 6,7,8,10,17 and 18 from the Australian Privacy Charter. These principles address freedom from surveillance, privacy of communications, private space, anonymous transactions, public registers, and no disadvantage;
- incorporating the Telecommunications Privacy Principle that privacy invasive technologies be accompanied by policies that preserve privacy at no additional cost to consumers;
- reflecting the fair information practices of the Québec *Act*;
- adding a requirement to inform individuals about information management practices as well as means of redress;
- adding a requirement for agents or subsidiaries to grant access to information directly rather than through the main business;
- adding a requirement for businesses to inform individuals of their range of operations, agencies and subsidiaries;
- requiring businesses that share information with agents, subsidiaries or third parties to ensure information is as accurate as that provided by the main business;
- ensuring the law covers all information uses by individuals, businesses, agencies, not-for-profit groups, churches, unions, political action/interest groups and others;

- clarifying consent, with expanded requirements for explicit consent, and more limitation on the use of negative option consent;
- requiring all non-essential marketing uses to be tied to an opt-out opportunity;
- requiring parental consent for the collection and use of children's information;
- limiting information collection to the absolute minimum required (which would eliminate gratuitous information collection);
- specifying that information only be collected directly from the individual;
- specifying that indirect information collection be allowed only in the rarest of cases and always documented, except in law enforcement situations;
- setting a minimum retention period for any personal information (at least six months to one year after last usage);
- specifying that, when information is corrected, all information accidentally or wilfully obtained that is not vital to operations be deleted;
- where a business refuses to change, add or delete information, requiring a correction request to be attached to the contested information and a list of third parties provided to whom the information was disclosed in the past two years;
- adding a reference to applicable standards for secure custody and disposal of information;
- incorporating special protections and restrictions on the use of biometric data;
- establishing a right of self-determination of health records (based on the Supreme Court Decision in *McInerney v MacDonald*), with this right to be inalienable and to apply no matter where the information is held in order to place greater custodial responsibilities on organizations that maintain data banks;
- prohibiting collection of unique identifiers except where specifically and legally allowed;
- prohibiting the transfer of information to other countries without adequate protection;
- requiring a contract making the Canadian organization liable for disclosure of personal information outside of Canada;
- ensuring all information sharing technology and programs, along with their purposes, are approved by government;
- requiring businesses providing services to government to be subject to the same obligations as the government body, and to public sector privacy laws;
- providing protection from fees and charges that could frustrate timely access to personal information;
- prohibiting eavesdropping and interception of information without the consent of both parties or a court authorization;
- requiring organizations to provide free summary listings of personal information used to provide services or make decisions, along with a fee structure to reflect the actual costs of providing full access;
- prohibiting surveillance except for law enforcement purposes;
- extending the same legal protections to e-mail as voice telecommunications;
- making it a violation similar to mail fraud to send SPAM (unsolicited junk e-mails) to people who don't want it;

- facilitating privacy protection through public key encryption to prevent mail-header forgery.

Highlights

It is generally agreed that the CSA Standard should be the basis for legislation. However, comments by various parties, including privacy commissioners, consumer groups, business organizations, special interest groups and individuals, on the need for greater precision and additional obligations should be considered in any drafting exercise.

2. Under what circumstances should the law permit disclosure of personal information to a third party without the consent of the individual? What conditions should apply?

Most parties who commented on this question feel the law should allow disclosure of personal information without consent for law enforcement as well as medical emergencies and other limited compelling circumstances when people are incapable of supplying their own information. Included in this category are cases of peril to health or safety, threats to others or self-injury, or where absolutely essential for business purposes (e.g. in cases, such as described by telephone companies, when personal information needs to be disclosed to ensure the effective operation of telecommunications networks). Risk to the environment is also suggested by the Information and Privacy Commissioner of Alberta and by one other party as a legitimate reason to allow disclosure without consent.

The use of personal data for medical research purposes elicited responses that disclosure without consent should occur only where there is a direct benefit to the individual or a clear "public good" as in research uses, with person-specific information available only where there is a direct benefit to the individual. There is little support for disclosure of personally identifiable health information without consent, except in rare circumstances. There is support for the idea that every disclosure for research purposes or in the public interest should require express individual or oversight body approval.

The archival community wants a carefully delineated exemption from consent requirements for historical material, while the Canadian Newspaper Association advanced strong views on the necessity for disclosure without consent for journalistic material.

Within the private business sector, many respondents feel the current wording within the CSA Standard is sufficient. Others want more clarity to deal with a number of specific situations, such as the collection and prevention of debt and, in the case of telephone companies, for business purposes such as customer win-backs.

Cable companies and ISPs want exemption from liability under the legislation when information is disclosed by a member of the public using their facilities, and when the information is not under their direct control.

Businesses that collect and use publicly available and business-related information about individuals want this information subject to disclosure without consent, saying it is often in the public interest to do so (e.g. there is a public interest in disclosing information concerning situations such as bankruptcy proceedings), while regulatory agencies such as securities regulators also want to collect and use information without consent to protect the integrity of the financial markets.

The insurance industry mentioned public duty responsibilities to disclose information without consent where the data is useful to public authorities to meet public objectives.

In contrast to these various examples, consumer groups generally want strict limits placed on disclosure without consent. There is only mixed support for disclosure without consent for journalistic purposes. The suggestion was also made that organizations be required to document and justify any disclosures without consent. Some of the varying positions are outlined below.

Privacy Commissioners

The federal Privacy Commissioner states disclosure without consent should only be allowed if the health and safety of the individual is at risk, or if required by law.

The Information and Privacy Commissioner of Alberta suggests disclosure without consent be allowed for law enforcement, for the health and safety of an individual, and for information about a risk to the environment, the health or safety of the public and when disclosure is clearly in the public interest.

Both the BC and Ontario Commissioners favour narrow and clearly defined circumstances for disclosure without consent. The Commission d'accès prefers the wording of the Québec *Act*.

Consumer Groups (including organized labour)

All groups that commented on this issue state that personal information should hardly ever be released without consent, citing law enforcement, emergencies and cases of peril to health or safety as the only grounds, based on an explicit, narrow and clearly defined public interest override. FIPA adds that specific probability of harm should be demonstrated.

PIAC adds that the law must also address the disclosure without consent of information in the public domain.

Health Care Sector

The CDA believes the law must allow disclosure without consent in specific health cases where a health practitioner has reason to believe the actions of a patient may cause harm (e.g. when dealing with patients with sexually transmittable diseases). In such cases, only the data specifically required should be released.

The CNA believes disclosure without consent should occur only where there is a direct benefit to the individual or a clear public good as in research uses, with person-specific information disclosed without consent only where there is a direct benefit to the individual. CIHI states that person-specific data should not be disclosed without consent except in specially defined situations. IMS believes no attempts to define exceptional circumstances would be comprehensive and wants the term "where appropriate" to be retained in *Principle 3* and added to *Principles 4 &* 5 of the CSA Standard.

Law Enforcement

The RCMP believes disclosure should require informed consent or that, at a minimum, individuals should be made aware that their information may be disclosed under specific and limited circumstances.

The RCMP adds that the legislative framework must allow disclosure to law enforcement agencies or other government investigative agencies (e.g. Customs, the Competition Bureau and Revenue Canada) based on Section 8 (e) of the current federal *Privacy Act* which permits disclosure without consent to "an investigative body specified in the regulations on the written request of the body, for the purpose of enforcing any law of Canada or a province or carrying out a lawful investigation, if the request specifies the purpose and describes the information to be disclosed."

Institutes

The U of O Centre recommends that the definition of consent include a statement that everyone has an inalienable right of ownership to their personal information, no matter where it is held.

Archivists/Historical/Library Associations

The Association des archivistes du Québec recommends a stipulation that consent be obtained for the use of sensitive personal information for a period of 20 years from the [illegible] of a document, extending to 75 years for sensitive personal information. Upon expiry of this period, individuals could also seek written authorization to keep personal information as personal property for a maximum period of 100 years from the date of the document.

CLARA recommends that guidelines for disclosure without consent follow those of the *Ontario Freedom of Information and Protection of Privacy Act* and the federal *Privacy Act*. The OLA wants disclosure without consent limited to specific scenarios such as threats to personal health and safety or when data has been stripped of all personal identity links.

The CHA/SHC believes disclosure without consent should address historical access to personal information about deceased persons, while the Institut d'histoire de l'Amérique française views the actions of obtaining consent, limiting the collection, use, retention and disclosure of personal information, and implementing security measures, accessibility and correction opportunities as being in direct contradiction to the activities related to history.

Telecommunications/Cable Sector

AT&T suggests that notifying individuals or seeking consent for disclosure should not be required in every telephone company transaction. The AT&T Companies expand on this by saying rules for disclosure without consent should follow generally accepted circumstances as indicated in the Québec *Act*, the federal *Privacy Act*, the *Telecommunications Act*, and current sectoral codes such as that of the Canadian Bankers Association. Sector-specific exemptions should be permitted, proposals for which should be registered with the federal Privacy

Commissioner. The AT&T Companies also suggest that telecommunications companies be allowed to share information about their customers without consent in case of emergency, and in the case of individuals who are in a debt situation (to prevent these individuals from running up large debts with more than one company). The AT&T Companies add that information sought pursuant to a legal power should not require consent and that legislation should take into consideration different business situations when defining the right to withdraw consent. The AT&T Companies view use and disclosure of personal information for purposes such as customer win-backs as legitimate business purposes which should not require further consent.

Microcell adds that disclosure without consent should be allowed to protect health and safety, for law enforcement, to protect against customer fraud, and to ensure that interconnected networks can operate efficiently. The CWTA position generally concurs with the Microcell view, adding that disclosure without consent should also be allowed where a third party, in the reasonable view of a service provider, is seeking personal information as an agent of the subscriber.

The CCTA notes that companies cannot be held liable for collection, use and disclosure of personal information by a member of the public involving the use of communications services and facilities provided by cable companies, where cable companies do not have direct control over the information. Rogers generally supports all of the positions stated above.

Financial Sector

CBA lists a number of specific situations where disclosure without consent should be allowed, including fraud, forgery, law enforcement, when the individual is a minor, seriously ill or mentally incapacitated, and cases where the data holder has an agent relationship with the third party providing related services. In these cases, a contract would be required to protect the personal information given to the third party. The CBO suggests disclosure without consent should be as per the current CSA Standard.

ACFC, Canada Trust, CLHIA, Equifax and ICC all support disclosure without consent as per the current CSA Standard. Canada Trust believes a sectoral code is the most appropriate place to provide more detail on disclosure without consent, and notes that disclosure without consent is required for agent relationships with third parties providing related services. ICC states that "public duty" should be added to the list, citing the nature of the relationship between P&C insurers and provincial motor vehicle registries that leads to the sharing of some information (e.g. claims-related data where there is a public interest) that is not strictly a legal requirement.

The Canadian Securities Commission, Canadian Securities Administrators and the Vancouver Stock Exchange (VSE) state that securities regulators need to be able to collect, use and disclose personal information without consent to carry out their mandate, which includes investigation of industry participants. The VSE calls for an exemption from legislation for the collection of information about members and listed companies, stating that individual access to this information should be denied in order to maintain public confidence in the integrity of

securities markets.

CGA Ontario says legislation should provide a short list of exceptional situations for disclosure without consent that would include disclosure with a search warrant or subpoena, if the information is already public, in the case of an emergency threatening health or security, and for legitimate research purposes where the information will not be disclosed to the public in a way that identifies the individual.

Commercial/Retail Organizations

Enlogix supports enumeration of circumstances as per the Industry Canada discussion paper. D&B believes strict limitations on disclosure without consent should only exist where information is normally considered confidential, noting that a great deal of information is by nature public and should be subject to legitimate public communication without consent. D&B notes that such public disclosure is essential in securities transactions and should be allowed in other cases where legitimate third party interests exist.

The CNA dismisses as ludicrous the concept that only those stories can be published wherein the subjects are pleased to consent to disclosure. CNA states that a clear exemption for journalistic purposes is required as use of the "except where inappropriate" clause in the CSA Standard (*Principle 3*) would only invite litigation.

Information Technology Associations

CAIP believes information should be disclosed without consent when there is a threat of self injury or a threat to others, with disclosure limited to a need-to-know basis. CAIP also states that a user policy or executed contract permitting disclosure without consent constitutes consent and should be recognized by law. CIPS would limit disclosure without consent to limited compassionate or compelling circumstances or situations where an organization is explicitly bound by law to disclose information. CIPS suggests disclosure without consent in law enforcement not include cases where law enforcement agencies are investigating their own employees. As well, private investigators should not be allowed to rely on legal provisions to seek disclosure without consent. CIPS also believes that, if disclosure of personal information without consent is to be an offense, it should also be an offence to attempt to gain access to such information without consent.

Individuals (including consultants, experts and academics)

Individuals had a number of suggestions on when disclosure without consent should be allowed, including:

- the current *Privacy Act*, section 8 (2) items *A* to *M* is a good starting point for a list, with a caveat that individuals be notified whenever there is disclosure without their knowledge and consent;
- the list should be more limited than the current *Privacy Act*, and disclosures without consent under court orders or judicial warrants should be brought to the attention of

the affected individual;

- disclosures for research, audit or statistical purposes should be allowed with approval from the federal Privacy Commissioner;
- disclosure without consent should only be when allowed by law in circumstances such as wiretaps;
- circumstances should be specifically delineated and indicate the benefit to the individual or the wider public interest;
- disclosure should be allowed where absolutely necessary in the operation of a business, with every disclosure logged;
- consent should always be required except in compelling circumstances such as danger to health or the safety of people, including environmental hazards (it was noted that, in order to protect privacy, health practitioners should not disclose an entire patient file when they are required to disclose patient information under law, such as knowledge of sexually transmittable diseases);
- disclosure without consent should be allowed by the media for news purposes;
- no one should be able to read e-mail without consent except by court order, and private companies should be required to inform employees when corporate e-mail is being monitored;
- an individual's rights to privacy should not be absolute and the community should have overriding rights to disclose information in instances such as addictive behaviour that disrupts a community.

Highlights

Various business organizations and other parties suggested specific categories of information use that should be subject to disclosure without consent. Other parties, including privacy commissioners and consumer groups want an extremely limited and highly specific list of information use categories and situations where disclosure without consent would be allowed. It was also noted by some parties that no such list can be exhaustive. In light of these differing positions, the best approach may be to include a well delineated list of examples of disclosure without consent within the legislation, and provide further guidance on circumstances under which such disclosures would normally be allowed. The suggestion made by a few parties that organizations be required to document and substantiate any such disclosures without consent is also worth consideration.

3. Should sectoral codes be recognized in the new law? If so, should they be binding? Or should they be used only to help interpret the principles of the law for specific sectors? Who should develop and approve them?

Many submissions acknowledged the value of sectoral and organizational codes in helping industry groups to interpret the CSA Standard. However, there was only limited support for binding sectoral codes under the law, especially for codes that would replace the legislation.

There were a few parties who would give sectoral codes legal weight by virtue of a government approval process. IMS Canada, the Canadian Dental Association, the Canadian Banking Ombudsman and the Canadian Direct Marketing Association all support legislated sectoral codes for all industry sectors and a national certification system. The Insurance Council of Canada wants sectoral codes to be binding on industry sectors and wants industry codes, therefore, recognized in law as having interpretative value when cases of non-compliance arise. Interpretative value means that in resolving disputes, setting penalties or awarding compensation, an oversight body must give due consideration to the organization's code and the manner in which this code was applied in determining if the law was violated.

The Public Interest Advocacy Centre suggests, however, that if sectoral codes do have any legal weight, they must at least meet, if not exceed the legislation, apply to an entire clearly defined sector, and be subject to public input.

The clear majority view is not supportive of binding sectoral codes replacing legislation or having recognized legal weight.

The positions of the various parties are outlined below.

Privacy Commissioners

Only the Information and Privacy Commissioner of Ontario supports the recognition of sectoral codes in the law. The Commission d'accès notes that no provisions exist for recognizing sectoral codes within the Québec *Act*.

The Ontario Commissioner states that sectoral codes should be recognized in law and binding as per the New Zealand model, noting, however, that the need for such codes will be quite limited if the legislation is well written. Binding sectoral codes should be reviewed by a number of parties including the responsible Minister, the oversight agency and an industry committee before being approved. The Commissioner warns, however, against ratification or grandfathering of existing sectoral codes developed before the presence of a law.

Consumer Groups (including organized labour)

Most consumer groups, including FIPA, BCOAPO, CAC, PIAC and Privacy Partners, along with CUPE, support the use of sectoral codes only as non-binding, interpretative documents.

CAC Ontario says such codes could be approved for use by the federal Privacy Commissioner but should not take precedence over legislation. BCCLA supports their use, providing there is funding for public interest participation in their development and consensus-based decision making. BCCLA believes such codes should have some official stamp of recognition indicating the development process was fair and inclusive, but not the authority of law.

FNACQ/OC sees such codes as being effective only if they are legally binding, and proposes that industry develop codes but the federal Privacy Commissioner verify them to ensure compliance with the law.

PIAC states that, if binding codes are allowed, they must equal if not exceed the legislation, should apply to an entire clearly defined sector, and the process to approve and enforce codes must include public input.

Health Care Sector

The CDA supports sectoral codes being recognized in law, as the organization believes specific privacy threats from corporate mergers, a variety of information gathering techniques and target marketing practices are too great to be left to self regulation. CIHI and IMS also want sectoral codes recognized in law. CIHI says they should be approved by groups knowledgeable about the sector and privacy laws. IMS states such codes should be certified and binding in the same way that adherence to the law is binding.

The CNA does not support the recognition of sectoral codes as a substitute for legislation.

Government (including the European Union)

The EU believes voluntary, non-binding codes are useful but less effective in isolation and more costly to implement and enforce.

Archivists/Historical/Library Associations

CLARA supports the use of sectoral codes as non-binding guides for tailoring the law and urges Industry Canada to encourage industry to include these codes in the National Library depository system, to make them accessible to the public. The CHA/SHC believes sectoral codes might be acceptable if they included far-sighted management policies. The OLA advocates the recognition of sectoral codes as binding where there is agreement among all stakeholders. OLA states that the proposed legislation, however, should supercede any sectoral code.

Telecommunications/Cable Sector

All respondents except AT&T support non-binding sectoral codes, developed and used for interpretation only. AT&T believes the government should outline requirements for codes which would then be developed by industry for review by the oversight authority. These codes would then be binding on the industries to which they apply.

Financial Sector

The CBA, CBO, CLHIA, Equifax, Deloitte employees and Canada Trust all support use of non-binding, interpretative sectoral codes, with Canada Trust suggesting that a reference to the role of sectoral codes be included in legislation. CLHIA does not support this last point, while Equifax states that legally binding provisions could be subsequently enacted if voluntary compliance proves to be demonstrably inadequate.

Only two organizations, ACFC and ICC advocate specific recognition for the interpretative value of sectoral codes in law. ACFC prefers a recognition of the interpretative value of codes that are non-binding. In this case, industry sectors would be required to develop and adopt codes, but approval under the law would not be required.

ICC also believes sectoral codes should be developed by the sector, without government involvement, but they should be certified by accredited independent auditors and registrars. They should then be recognized in law as binding on the industry sector. ICC states that codes recognized in law as binding on an industry will lead to greater certainty and predictability in how oversight is applied.

CGA Ontario favours the New Zealand model, under which binding industry codes require public sector input and federal Privacy Commissioner approval, with some method for the Privacy Commissioner to [illegible]e their review and revision if circumstances warrant.

Commercial/Retail Or[illegible]izations

The CDMA believes sectoral codes should be registered with a national body and certified as meeting the CSA Standard, while D&B suggests, based on the limited industry experience with voluntary codes, that it is premature to judge how sectoral codes should be integrated into legislation. Enlogix does not think sectoral codes should be binding, and the CGA sees no need for sectoral codes or guidelines within the natural gas industry.

Information Technology Associations

All organizations in this sector support non-binding sectoral codes, used for interpretation and guidance only.

Individuals (including consultants, experts and academics)

Individual opinion on the value of sectoral codes ranges from no support at all (a "waste of time") to a view that they should be non-binding and used for interpretation only.

Only two individuals believed sectoral codes should have any formal recognition. One health care practitioner said they should be recognized in law where groups such as medical ethics committees must regulate over professional bodies to protect the public, and exercise powers to sanction members and assess penalties. Another individual said they should be developed by industry and associations and verified by recognized professional bodies.

Highlights

There is limited support for binding sectoral codes, and it is generally suggested by respondents that there be no provision within legislation to allow sectoral codes to replace legislation or have legal recognition, including interpretative value. One business submission, in particular, raised the issue of the interpretative value of such codes (i.e. courts, in determining penalties or awards would have to give due consideration to the manner in which the organization interpreted the legislation within its sectoral code). One consumer submission, however, suggested that a fundamental reason why greater precision is required within the legislation is to prevent organizations from using the "impenetrable defense" that they have applied subjective judgement to the CSA Standard in good faith. Perhaps, given these conflicting views, the question of interpretative value is best left to the courts without any direction within legislation.

4. Should some types of information be excluded from the scope of legislation? If so, in what circumstances?

This question elicited specific and detailed comments from only a few respondents. The federal Privacy Commissioner and the Alberta Commissioner do not want any exclusions while the BC Commissioner wants the law tightened even further to include biological information such as tissue samples. There are mixed views on journalistic exclusions.

Among others who commented on this question, there was mixed support for completely excluding journalistic material. One individual suggestion was that this issue be dealt with similarly to the EU Directive which excludes such material from some provisions of the Directive, but not all.

There were also suggestions that information of an entirely personal and non-commercial nature (e.g. a personal telephone directory or photo album) should be excluded.

One suggestion worth highlighting is that the definition of "person" under the law should extend to "natural persons" only, so as not to convey privacy rights to corporations.

There were mixed concerns about how far information already in the public domain should be excluded (if at all) since there are notable differences between widely available public domain information and information that, while available, is generally not intended for widespread distribution or use. As described below, there are also many other noteworthy exclusions sought by business organizations.

Privacy Commissioners

Privacy commissioners generally believe there should be no exclusions or they should be extremely limited. The Information and Privacy Commissioner for BC believes the range of information subject to the legislation should be extended to capture biological information such as tissue samples. The Information and Privacy Commissioner of Alberta does not advocate excluding any information and the Information and Privacy Commissioner of Ontario does not advocate exclusion of journalistic material. The Commission d'accès does support excluding the collection, retention, use and disclosure of personal information for journalistic purposes as per the Québec *Act*.

Consumer Groups (including organized labour)

This question was only directly responded to by three organizations, with the focus largely on journalistic material. The CAC opposes any exemptions, including for information collected and used for journalistic purposes. FNACQ/OC believes journalistic material should be exempt as per the Québec *Act*. FNACQ/OC also believes information used for artistic purposes should only be exempt where the individual involved could not reasonably expect protection and where all efforts have been made to obtain consent. FIPA believes exemptions should exist for journalistic material, and judicial and ecclesiastical records, as well as

information compiled and used for purely personal purposes. FIPA adds that personal information in archival material could have a carefully delineated and limited exemption.

Health Care Sector

Both CIHI and IMS Canada want non-identifiable data excluded from the law.

Government (including the European Union)

The EU cautions that it has not found it wise to exclude certain types of data processing entirely from the scope of legislation. In their view, a more appropriate balance would be to exempt data processing activities such as journalism from certain principles.

Archivists/Historical/Library Associations

The Association des archivistes du Québec believes that files and documents of a personal nature that are stored manually are naturally protected and, therefore, should be exempt from legislation as long as the information is not collected specifically on an individual and the document is not computerized. The CHA/SHC also urges exemption of data of a historical nature, while the OLA wants all data to be exempt where links to individuals have been removed.

Telecommunications/Cable Sector

The CWTA believes there should be no exemptions while Microcell would exclude journalistic material and suggests there may be a need to exclude information used to ensure the security of public key-based encryption systems.

The AT&T Companies believe that, within the telecommunications sector, companies acting in the role of a carrier or service provider should be exempt from any accountability for the use made of communications facilities by customers. Legislation should not require businesses to seek to gain control of or to protect information not under their control by virtue of the products and services they provide. Rogers supports this position and adds that information not attributable to an identifiable individual be exempt, such as information traceable only to an Internet protocol (IP) address, not an individual. Similarly, Rogers would exempt Internet usage information compiled in aggregate form which may be used for marketing purposes.

Financial Sector

CBA states that the scope of legislation should be limited to information about natural persons, and that proprietary information should be excluded so as not to jeopardize the competitive positioning of business organizations. CHLIA favours exclusions as per the current CSA Standard. ICC proposes that information about non-identifiable individuals be exempted.

The Western Forum of Credit & Financial Executives cites the requirement for credit agencies to retain information for long periods of time in order to combat the misuse of credit and credit fraud. The Forum adds that overly broad definitions of personal information in the CSA Standard coupled with onerous consent requirements could lead to censorship of data under

the guise of privacy protection, with harmful effects to the credit industry. The Forum, therefore, calls for personal information now governed by provincial credit reporting, debt collection and other related legislation to be exempted from privacy legislation, as well as information used for the initiation, extension and collection of credit. The Forum adds that information for business contact purposes should be exempted and record-keeping for ongoing business purposes should be considered the private property of the firm lawfully obtaining the data.

Equifax also proposes exemption of consumer credit information since it is already subject to provincial laws, stressing that such an exemption is particularly necessary if harmonization of various jurisdictions cannot be achieved.

Commercial/Retail Organizations

Enlogix advocates that all statistical or aggregated data be excluded from the scope of legislation if it cannot be rendered personal again through manipulation. D&B believes information gathered about business entities should be excluded from legislation and that the legislation should apply only to natural persons.

The CNA believes information gathering for the purposes of journalism and newspaper archival material should be exempted from the scope of legislation to protect constitutional values.

Information Technology Associations

CAIP states that the same conventions that apply to other forms of communications should apply to e-mail, and any party who legitimately receives personal electronic messages should be able to reveal the contents and any electronic header information (i.e. Internet Protocol addresses) without fear of reprisal. CAIP also believes on-line businesses should not be regulated more than other commercial enterprises and, thus, ISPs (only some of which may be subject to federal privacy legislation) should be able to use subscriber electronic header information for marketing purposes, and to rent and sell to other organizations, much as magazine publishers do with subscriber lists.

CIPS is concerned about treatment of records within the public domain and questions whether any exclusion of such records should apply to individual records only or an entire database. CIPS also believes legislation needs to address whether an organization can use a public record for purposes other than those for which it was originally compiled. Also at issue is whether organizations should be able to use public records created for one regulatory purpose to fulfil another regulatory purpose.

Individuals (including consultants, experts and academics)

Eight individuals commented directly on this question and their comments reflect both general and specific concerns about exclusions. One individual states there should be no exclusions; another wants no exemptions that would relieve business of the legal responsibility to protect customer and employee privacy. Another individual adds that the law should apply

equally to employee and customer information, and employees should not be required to sign away privacy rights with waivers in employment contracts. However, a contrary view from one health care practitioner is that organizations that use limited amounts of data should be allowed to register and define how they would apply the CSA Standard (e.g. be exempt from legislation), while institutions that collect and use a great deal of personal information would be subject to a specific, enforceable law.

Another health practitioner believes groups such as researchers should be able to apply for an exemption from subpoena for any particular research information and wants information such as cancer registries, Statistics Canada mortality and morbidity files, and hospital admission and separation files treated in a different context than private sector business information.

One individual states that data that has been rendered anonymous should be excluded and freedom of the press needs safeguarding. This was supported by one journalist who adds that the law should apply only to organizations, not natural persons (including free-lance journalists). Another individual opposes exclusion for journalistic material, but states that information about any individual who has been deceased for two years, information for strictly private and non-commercial uses, and information from widely known and accessible sources such as telephone directories should be excluded.

Highlights

The submissions indicate that the legislation should define "person" to include only natural persons to avoid giving organizations the information protection rights of individuals. The drafters of legislation should also consider whether to distinguish between widely available public domain information and public information that is not intended for widespread distribution or use. Where categories of data users seek exemptions from the legislation, the drafters should consider whether to exempt users from the full scope of the legislation or whether exemptions, if any, should be restricted to particular aspects (e.g. an exemption from the obligation to obtain consent before information collection, use or disclosure).

Powers

5. Do you favour start-up obligations such as a registration scheme to ensure compliance with the law? If so, which approach do you favour? Who should be responsible for overseeing privacy protection?

The majority of respondents see little value in or are opposed to complex registration schemes. No privacy commissioners support the concept as do few business respondents. There is limited support for the mandatory filing of codes and contact information with the federal Privacy Commissioner or other public body. This view is supported by the AT&T Companies, Stentor, and the Association of Canadian Financial Corporations.

Most consumer groups, however, do support start-up registration of some type, as do two individuals. The main purpose and support for such registrations is generally to establish a central repository of codes and contact individuals. Specific views are outlined below.

Privacy Commissioners

Privacy commissioners are unanimously opposed to start-up obligations such as registration, calling such regimes cumbersome and expensive, unnecessarily bureaucratic and possibly counterproductive. In general terms they note that since data commissioners around the world have frequently been tasked with running registration systems, this community is well placed to comment on the effectiveness of such schemes.

Consumer Groups (including organized labour)

Of eight consumer groups that responded to this question, three oppose mandatory start-up registration and five support it.

Privacy Partners supports it, but says the process should not be onerous for non-profit organizations and small business, but should instead lead to easy access to information on organizational practices and policies. PIAC says registration will help identify "high risk" data users, as well as identifying and monitoring inappropriate and inadequate practices. The registry should be maintained by the oversight body which should have the resources to properly review filings and conduct follow-up activities ranging from phone calls to full audits. A registration fee would help fund the oversight body's education and oversight activities. All companies that deal with personal information would also have to report annually and make public information on complaints handling.

CCC and CAC Ontario also support registration, as does CAC which calls for registration schemes suitable for the size of the business and the sensitivity of the information, with third party verification by Standards Council of Canada (SCC) accredited privacy registrars as the norm. The legislation should specify when self-registration would be allowed, such as for small businesses or for non-sensitive information.

Health Care Sector

Only CDA supports mandatory registration, adding that some sectors dealing with vast amounts of personal information may require specific enforceable legislation. CIHI suggests registration with the CSA or the federal Privacy Commissioner could be voluntary.

Archivists/Historical/Library Associations

Neither CLARA nor the OLA support a start-up registration scheme. Other organizations are silent on this issue.

Telecommunications/Cable Sector

There are only two comments in support of any form of registration. The AT&T Companies support registration of sectoral codes with an oversight body, as well as providing the name of the organizational contact responsible for administering codes. Stentor believes registration can be useful, but companies should be free to employ it where they see fit. Stentor also suggests that tailored codes, along with the name of the contact person, could be filed online with a government web site.

Financial Sector

Most respondents who commented on this issue do not support start-up obligations or registration. ICC suggests compliance to a code should be assumed in the absence of complaints or any compelling evidence to suggest a problem with personal information protection. CBO states that, in order to support its model of maximum industry self-regulation, codes should be audited by accredited privacy examiners.

ACFC suggests a requirement to file codes with the federal Privacy Commissioner, which it deems to be a cost-effective alternative to registration. Equifax states it is not opposed to voluntary registration and suggests such schemes could become compulsory if there is evidence of a high level of non-compliance.

Only Deloitte employees support start-up registration with initial audits. Audit results would be reported back to a sectoral body and passed on to an oversight agency for monitoring. The sectoral body should periodically review privacy policies to ensure they remain current in a changing technological climate.

Commercial/Retail Organizations

Enlogix favours start-up registration, with tailored codes approved by an accredited body under the SCC or a government body under legislation. Industry should develop such codes with CSA or government guidance. Any initial or subsequent audits should be performed by accredited third-party auditors, not government, and should not be mandatory.

The CDMA also supports registration of codes. The CGA, however, is opposed to registration and states that, if a registration scheme proceeds, utility companies should be exempt

to reduce regulatory burden. The CGA also believes federal privacy law would be an intrusion into property and civil rights matters constitutionally under provincial jurisdiction.

Information Technology Associations

No organizations support start-up obligations such as registration. CIPS supports a "self-declaration of compliance" which is subject to challenge by third parties and review by the oversight body. In return for self-policing ability, companies should be required to keep rigorous records to demonstrate compliance.

Individuals (including consultants, experts and academics)

Seven individuals commented on this question, of which four do not support start-up obligations. Of the rest who support them, one wants a privacy registry data base where mandatory registrations could be self-filed and publicly available via the world wide web. Another suggests voluntary registrations may serve as evidence of compliance with the law and would, therefore, minimize the amount of verification or auditing necessary by the federal Privacy Commissioner.

One individual suggests businesses planning to use intrusive technologies such as biometric identification or smart cards should be required to register or be licensed by government.

Highlights

Support for registration procedures, where it exists, seems to be on the merits of creating a central repository of codes and contact individuals. Given the lack of support for this concept from privacy commissioners, and the availability of such information directly from organizations under the law, a registration process appears to be unnecessary.

6. What powers are needed to investigate cases of non-compliance and resolve disputes about the terms of compliance?

Generally, all parties commenting on this issue recognize the need for investigative powers when a complaint arises. However, not all parties provide a detailed listing of those powers required to conduct an investigation. Where detailed powers are mentioned, they are generally in line with the existing powers of the Privacy Commissioner. Specific comments are outlined below.

Privacy Commissioners

The federal Privacy Commissioner lists existing powers under the current *Privacy Act* along with additional powers, including the ability to impose fines if investigations are wilfully obstructed, a power to refuse to investigate or to abandon a complaint under certain circumstances, and a power to initiate and receive complaints directly. Powers are also required to approve and monitor disclosure of personal information for research and statistical purposes.

The Information and Privacy Commissioner of Alberta believes the oversight body must have powers to respond to complaints and investigate on its own initiative, have full rights of entry and access to information, audit records and information management systems, mediate disputes, set deadlines for response, hold hearings, examine witnesses, issue binding orders, and impose penalties for wilful obstruction. The oversight body should also be able to comment on the privacy implications of new technologies, services or programs, and oversight agency personnel should be protected from proceedings while performing legislated functions.

The Information and Privacy Commissioner for BC believes the powers should be those of the existing federal *Privacy Act*, with the necessary regulatory powers to settle disputes that proceed beyond industry dispute resolution procedures. The Information and Privacy Commissioner of Ontario lists a full range of powers similar to those listed by the Alberta Commissioner, with the addition of powers to issue binding orders with full and effective remedies.

The Commission d'accès recommends powers as per the Québec *Act*.

Consumer Groups (including organized labour)

CPI recommends a complaints-driven model only, in which consumers and business are both made aware of their rights and obligations. If consumers are not satisfied with the outcome of their complaints to business, then an independent investigation can take place. All investigation reports from the oversight body should be publicly available from the organization being investigated, similar to a Better Business Bureau approach to customer satisfaction.

All other consumer organizations support more proactive investigative powers. FIPA suggests powers similar to those found in provincial privacy legislation. PIAC details the fullest range of powers of all responses. In addition to powers already noted, these include: the power to

make all investigation and audit results public; express legislative powers to delegate certain investigative/audit functions to qualified third parties; the power to make industry regulations governing practices and procedures; the power to charge fees to data users; the power to impose penalties for non-compliance and issue remedial orders. PIAC adds that individuals should also be able to require mandatory investigation by the oversight body based on the six adult person threshold established under S.9 of the *Competition Act*.

Health Care Sector

IMS Canada says the law requires powers to demand periodic internal or external audits, and the CDA calls for powers to review, audit and discipline.

Government (including the European Union)

The EU suggests an independent oversight authority must have powers to verify compliance with the law even in the absence of complaints.

Institutes

The U of O Centre believes privacy commissioners should have powers to receive, investigate and settle complaints of alleged privacy violations.

Archivists/Historical/Library Associations

CLARA believes powers should be consistent with those of the Information and Privacy Commissioner of Ontario and include the powers to investigate non-compliance, obtain copies of records, require information to be submitted under oath, and both issue and publish recommendations to improve compliance and conduct follow-up investigations.

The OLA suggests organizations deal with complaints first and be required to report the complaint and the resolution to the federal Privacy Commissioner. The Privacy Commissioner's powers should be limited to the investigation of actual violations.

Telecommunications/Cable Sector

The AT&T Companies suggest the oversight body should be restricted to receiving complaints and should rely on self-regulatory organizations to resolve these complaints, while monitoring compliance and undertaking investigations and research as required. There should be a statutory duty to meet with and mediate between parties to any given dispute.

Stentor also supports a complaints-driven process in which companies and individuals attempt to resolve disputes first, with the oversight body having powers to investigate disputes, mediate between parties and make recommendations for improving practices where disputes cannot be resolved directly between the parties.

The CWTA concurs with this approach and adds the legislation must clearly indicate the principles to be respected in investigating any alleged privacy violation. The CWTA says that

any decisions arising from investigations should be accompanied by reasons for a decision, and proper legal procedures must be followed to gather information.

The CCTA and Rogers, which favour continuing oversight by the CRTC, state that the current CRTC powers to inquire into matters, hear evidence, determine facts and make mandatory decisions are sufficient to protect personal information.

Financial Sector

CBA and the CBO believe the primary responsibility for privacy oversight must rest with sectoral organizations. CBO says that, where industry-managed sectoral bodies exist, the sectoral oversight body should only make non-binding recommendations to the dispute parties when disputes cannot be resolved. The sectoral oversight body should, however, be required under legislation to report publicly on complaints received and how they were resolved. CBO believes that the threat of such public reporting should be a sufficiently persuasive mechanism to make any recalcitrant business follow the recommendations.

Canada Trust and Equifax also suggest the greatest reliance should be placed on industry-led mechanisms. Canada Trust says the powers of an oversight body should include a role of policy advisor, as well as reviewing company codes and processes in the infrequent cases where issues remain unresolved.

Equifax calls for limited investigative powers and no proactive inspection powers. The oversight body should be required to refer all complaints first to the business or entity involved, with subsequent power to refer complaints to provincial oversight agencies where entities are subject to provincial jurisdiction. Only when all such processes are exhausted should an individual have the right to appeal to a national oversight body.

ICC supports oversight powers to conduct investigations and inspections where appropriate, but with clear limits. In ICC's view, in the absence of a complaint, investigation should only be authorized where there are reasonable grounds to believe the law is being breached. ICC also states that current federal Privacy Commissioner powers suitable for the public sector, including powers to publicize findings, could lead to well-intended but wrong orders with severe and unintended consequences for P&C insurers.

CGA Ontario calls for broad powers of enforcement, including the power to audit information use practices, to make specific orders pertaining to a business and general orders pertaining to broader, industry-wide problems. Legislation should specify that these latter powers be used only in exceptional circumstances, and industry should be able to apply for some form of judicial review for both specific and general orders.

Deloitte employees favour powers provided within a legal framework for sectoral oversight bodies, such as industry associations, to demand third-party audits and investigations, including examining witnesses, requiring testimony, ordering the production of documents and

arbitrating decisions. The results of this audit process could be appealed by the complainant to the sectoral oversight bodies or a government legislated oversight body, whose decisions would be binding. Violations of the code should be publicized as an incentive for organizations to comply with the law.

Commercial/Retail Organizations

The CGA proposes complaints-based investigative powers only, based on an oversight model closer to an ombudsman than a regulatory agency. Legislation should also allow the oversight agency to delegate powers and responsibilities to other jurisdictions and to assign complaints to existing processes. There should be time limits for investigations with safeguards against frivolous or repetitive complaints.

Enlogix supports ombudsman-like powers of investigation and audit. The CDMA reserves comment on enforcement measures until more details about an enforcement regime are publicly available.

Information Technology Associations

CATA, CAIP, and ITAC support complaints-based enforcement only. The Advanced Card Technology Association of Canada recommends broader powers, suggesting that site visits and audits by the oversight body are useful as remedial, rather than confrontational tools. CIPS says the oversight body needs the powers to compel organizations to produce evidence, and says it should be an offence to mislead or attempt to mislead the oversight body.

Individuals (including consultants, experts and academics)

Individuals generally seek proactive powers as per the powers currently available under the federal *Privacy Act*, including the powers of audit (two suggestions are that these powers should be equivalent to those of Revenue Canada or human rights commissioners).

There were two additional comments that these powers should either be used only to address the most serious complaints, much as the misleading advertising provisions of the *Competition Act* are handled, or where sectoral bodies have exhausted their processes or are likely to fail.

Highlights

Generally, all parties recognize the need for investigative powers when a complaint arises. Where detailed powers are recommended, they are generally in line with the existing powers of the federal Privacy Commissioner.

7. What powers are needed to address violations of the law and compensate individuals who have been harmed?

Consumer groups and privacy commissioners favour broad powers to address violations. Most parties support the power to publicize consumer complaints and non-compliance, without fear of liability, and some suggest this is one of the most important deterrent powers.

Consumer groups stress that fines should not simply become a cost of doing business. They should be set high enough so as to remove any business benefit of violating the law. Most business respondents feel that compensation should be left up to the courts with fines commensurate with actual damages. Specific comments are listed below.

Privacy Commissioners

The federal Privacy Commissioner supports a complaints model that encourages individuals to deal directly with organizations first. However, where there is evidence of non-compliance and harm to the individual, the Privacy Commissioner should have the ability to identify appropriate redress for the complainant. If an organization fails to implement recommendations made by the Privacy Commissioner, the Commissioner should have the power to publicize this fact. The Commissioner should also be able to refer matters to the Federal Court where compliance could be ordered, fines could be set and individuals could be compensated.

The Information and Privacy Commissioner of Alberta believes the federal Privacy Commissioner requires the powers to impose penalties and sanctions for wilful obstruction, determine issues of fact, find merit in complaints, grant remedies and award damages, limit liability in class action cases, and apportion liability between data users and processors.

The Information and Privacy Commissioner for BC proposes penalties and sanctions under criminal and civil processes, and the Information and Privacy Commissioner of Ontario proposes powers to require an organization to change or cease an information use or practice, and order the destruction of information. The federal Privacy Commissioner should also have the power to file an order with the Federal Court, making it a court order for enforcement purposes. In rare cases where an individual has truly suffered harm, the Privacy Commissioner should be able to award compensation.

The Commission d'accès suggests fines be established as per the Québec *Act*.

Consumer Groups (including organized labour)

Privacy Partners believes the oversight body needs the powers to publicize names, order audits, order third party investigations of policies and procedures, and set fi s and award compensation.

CAC adds that penalties should be stiff and escalate with repetition. They should be

levied in reference to the offender's gross annual income and, where violation of privacy law is for personal gain, be related to the anticipated gain. PIAC supports this position, adding that every day an offence continues after notification should be considered a new offence. PIAC states that compensation should be provided for distress, annoyance and embarrassment. Designated offences should include failure to register, failure to report, and failure to submit a privacy impact assessment. Under the federal *Contraventions Act*, these should be considered strict liability offences in provincial courts.

PIAC adds that private citizens as well as the oversight agency, through the Attorney General, should have the right of criminal prosecution or for injunctive relief, both interim and final. The law should also set limitation periods on prosecutions in a way that will not hamper law enforcement ability. In addition, restitution orders should give prosecutors first call on court-imposed fines to recover costs, with a 50% award of any fine to the successful private prosecutor. Civil suits should be actionable by individuals as well as in class actions and State (substitute) actions. These actions should be pursuable in small claims court with damages awarded for distress, annoyance and embarrassment, a minimum recovery rule of $500, and an onus on the defendant to prove due diligence. Successful plaintiffs should be able to cover their legal and investigatory costs.

FIPA generally endorses the powers noted above and adds the oversight body should have the powers to approve or forbid indirect collection of personal information. FNACQ/OC endorses the powers noted within the Industry Canada discussion paper, and the BCCLA supports compensation as per precedents set in other administrative law contexts.

CUPE supports broad powers to enforce legislation, including the power to investigate, make binding orders, impose penalties, make remedial orders and order compensation.

Archivists/Historical/Library Associations

CLARA recommends a provision for fines in the legislation for wilful or deliberate violations of the law, while the OLA calls for legally binding enforcement and penalties in the same way as environmental violations are handled.

Telecommunications/Cable Sector

AT&T believes there should be consequences for failing to comply with fair information practices, but cautions that a public listing of non-compliant companies could have a significant negative impact on business. The CWTA believes the oversight body should only issue non-binding recommendations regarding complaints and concerns and, if action is not taken, the issue could be furthered resolved by the Federal Court. The CWTA says powers to address violations and compensate individuals are best left to the courts. The AT&T Companies and TELUS also believe enforcement and compensation powers should reside with the courts.

Stentor supports an oversight body's power to publicize findings, subject to an appeal mechanism prior to publication, but believes parties should be able to test issues of law or

jurisdiction before the Federal Court, and that provincial courts should resolve compensation issues.

Rogers supports powers to order specific performance, injunctive relief and limited fines to address violations of the law.

Financial Sector

The CBO believes that sectoral oversight bodies should have only the power of recommendation and the power to report publicly on how complaints were disposed of as an inducement to business to comply with the legislation. The CBO prefers a non-binding process and cautions that the principles of natural justice must apply to any binding decision-making powers given to a government oversight body.

CHLIA wants penalties and compensation dealt with in a manner consistent with the treatment of other aspects of market practice and consumer protection, while ACFC states that penalties and compensation are best left to the courts, which are familiar with the right to privacy as a civil right. Equifax, which is subject to provincial jurisdiction, notes that some, but not all provinces have legislation establishing the tort of invasion of privacy and many provincial courts have recognized this tort by common law jurisprudence.

ICC believes compensation for damages should only be awarded with proof of damage, and only to the extent that the company that breached the privacy law cannot first correct the damage. In many cases, the appropriate remedy would be for the company to correct the information and communicate corrected information to third parties where necessary.

CGA Ontario believes monetary compensation is best left to the courts, while the privacy legislation should provide for a statutory right of civil action similar to the United Kingdom *Data Protection Act, 1984*. Issues to resolve are whether business would have a defence to such an action based on taking reasonable measures under the *Act*, and what damage awards would be available if no actual damages could be proved.

Deloitte employees do not favour compensation for damages since this would only encourage complaints. Fines and publicizing of violations should suffice as deterrents.

Commercial/Retail Organizations

The CGA says there is no need to strengthen existing privacy laws with regard to violations and compensation. Enlogix proposes powers of mediation and recommendation, but does not support coercive powers.

Information Technology Associations

The Advanced Card Technology Association of Canada believes the federal Privacy Commissioner should be the ultimate oversight agency with powers to both impose penalties appropriate to the offence and award compensation to victims, commensurate with damages

suffered. CIPS supports powers to make binding orders through a tribunal to rectify non-compliance and to compensate individuals.

Individuals (including consultants, experts and academics)

Individuals who commented on this question have mixed views on the powers that should be available to address violations and compensate individuals. One wants limited sanctions available, but believes compensation should be handled separately. Another wants the judicial system to address violations and compensate. A third prefers a national model similar to Revenue Canada with powers to investigate and fine all business organizations, regardless of jurisdiction. A fourth states the powers should be as per existing privacy commissioners. There is also a comment that there should be mediation and arbitration powers to address small and honest errors without invoking an excessive level of intervention.

Of those who offered more specific comments on powers (four individuals), there is common agreement on the need for powers to make binding orders, award compensation and levy fines. One individual calls for powers to order cessation of organizational practices that violate the law and to force remedial corrective action with follow-up audits, as well as making offenders issue public apologies and publish details of violations. One individual suggests companies be prohibited from selling services for a defined period.

Where fines are mentioned, the view is that they should be in proportion to the size, nature and potential damages, and should be set high enough so that deliberate misuse of personal information not to become a cost of doing business. Another calls for fines payable to the wronged person of up to $100,000 and imputable to either the business or an individual employee.

Highlights

Consumer groups and privacy commissioners favour broad powers to address violations. Most parties support the power to publicize consumer complaints and non-compliance, without fear of liability, and several business and consumer groups as well as individuals suggest this is among the most important deterrent powers

8. Should there be powers to conduct independent research and proactive investigation/inspection of an organization's practices and to write reports?

There is general agreement that oversight bodies should have powers to conduct independent research *of a general nature*, since such research on new technologies and emerging privacy issues is of value to all parties.

There is, however, mixed support for proactive investigations of organizations. Most business submissions oppose proactive investigations. Among consumer groups, the CAC calls for investigative powers to act on suspicions and PIAC calls for the six-person threshold of the *Competition Act* (s.9) to be the basis t force a mandatory investigation by the federal Privacy Commissioner. The federal Privacy Commissioner suggests powers to conduct an issues-based audit where multiple complaints, investigation and mandatory mediation suggest systematically inadequate information practices. Other privacy commissioners support a similar position. Detailed comments are outlined below.

Privacy Commissioners

All privacy commissioners support powers to conduct independent research and proactive investigation and inspection.

Consumer Groups (including organized labour)

FIPA supports a complaints-driven model while all other organizations commenting on this issue generally support proactive powers, including powers to act on suspicions or rumours.

Privacy Partners notes, however, that only 15% of respondents to its survey feel the law should allow a company to be investigated at any time to make sure it is obeying the law, without the basis of a complaint.

Health Care Sector

CDA supports proactive powers of investigation, stating that privacy protection should be more than complaints-based.

Institutes

The U of O Centre believes privacy commissioners should be able to initiate investigations via privacy audits and technology impact assessments, and also carry out studies relating to privacy and emerging technologies.

Archivists/Historical/Library Associations

The OLA believes that powers to conduct independent research and investigation should be limited to actual violations of the law, as well as research and statistical reporting on data stripped of links to actual identity.

Telecommunications/Cable Sector

The AT&T Companies do not support proactive powers to inspect and investigate organizations, but do support independent research. Rogers and Microcell also claim proactive investigative powers are unnecessary and that investigation should be on a complaints-basis only. Microcell also recommends that the legislation should recognize the costs to organizations of investigations and inspections and allow those costs to be recoverable in the event an investigation is unfounded. Stentor companies do not oppose a requirement to report complaints received by companies, provided such reporting is done on a routine and purely statistical basis.

Financial Sector

The CBO, ICC and Equifax do not favour proactive investigation and inspection of organizations' privacy practices, stating that oversight should be complaints-driven. An oversight agency should be able to report, however, on systemic problems, monitor industries, examine new technologies and engage in public education.

CHLIA says only that the oversight model must be consistent with the treatment of other aspects of market practice and consumer protection.

Deloitte employees state only that an oversight body have monitoring powers. CGA Ontario supports audit powers and believes the oversight body should have the power to assess new technologies.

Commercial/Retail Organizations

The CGA supports complaints-based powers only. There were no other direct comments on this question .

Information Technology Associations

The Advanced Card Technology Association of Canada supports independent investigations such as site visits and audits. Other organizations are silent on this issue.

Individuals (including consultants, experts and academics)

All individuals who commented on this question support proactive powers of investigation.

Highlights

There is broad agreement that oversight bodies should have powers to conduct independent research *of a general nature*, since such research on new technologies and emerging privacy issues is of value to all parties. Most business submissions oppose proactive investigations, while privacy commissioners, consumer groups and individuals support broader powers to conduct investigations where multiple complaints, investigation and mandatory mediation suggest systematically inadequate information practices.

Distribution of Powers and Responsibilities

9. Should a central oversight authority be established to oversee the implementation of the new legislation, and if so, what powers should it have? Should this role be added to the responsibilities of the federal Privacy Commissioner or some other body?

The vast majority of respondents favour the use of the existing Office of the Privacy Commissioner as the oversight body.

There were a few alternate views put forward by specific industry groups. The cable television industry advocates continued use of their existing self-regulatory model under CRTC oversight. One respondent from the credit industry wants this industry to be exempt from legislation. Other regulated organizations subject to provincial legislation stressed their preference for continued oversight by provincial sectoral regulators.

10. Should a tribunal be established, or should a higher court be given the task of issuing binding decisions on complaints?

Overall, there is a slight preference for use of the Federal Court over tribunals. The use of the Federal Court may be even more favorable if processes, such as those suggested by PIAC (*see Question 7*), are put in place to make provincial courts (e.g. small claims court) more accessible for small actions. Specific views are noted below.

Privacy Commissioners

The federal Privacy Commissioner and the Commission d'accès support the use of the courts for binding decisions. The Commission d'accès notes this is currently the practice under the Québec *Act*.

The Information and Privacy Commissioner of Alberta prefers a tribunal to make final and binding decisions, stating that the courts are already overburdened. The Information and Privacy Commissioner for BC says that sectoral bodies such as the CDMA could make the initial decisions on privacy disputes with the federal Privacy Commissioner having final binding powers. Judicial review of Privacy Commissioner decisions should, however, be available on grounds of error in law, bias, absence of jurisdiction, and other administrative law issues. The Federal Court should hear such a review.

The Information and Privacy Commissioner of Ontario believes the federal Privacy Commissioner should have binding powers, but that a second, undescribed, level of appeal should be available in cases where compensation and restitution are awarded. The Ontario Commissioner says the ability to appeal decisions awarding compensation is appropriate.

Consumer Groups (including organized labour)

FIPA, PIAC and FNACQ/OC prefer the use of the Federal Court, with FNACQ/OC adding that the establishment of a tribunal such as the tribunal under the *Canadian Human Rights Act* is another option.

The CCC, CAC Ontario, BCCLA and CUPE support the use of a tribunal to issue binding decisions over use of the courts. Privacy Partners says, however, that the legislation should specifically state that nothing within the law prohibits individuals from using other remedies such as criminal charges and civil remedies.

Health Care Sector

CDA's view is that, with a sectoral self-regulation model, the federal Privacy Commissioner would be the tribunal of last resort.

Government (including the European Union)

The EU prefers courts and judicial review to tribunals.

Archivists/Historical/Library Associations

CLARA cites the Information and Privacy Commissioner of Ontario's role as a tribunal with the power to issue binding decisions as an efficient model, and states there is no need to establish an additional tribunal. The OLA advocates a tribunal be established as part of the Office of the Privacy Commissioner. This tribunal would resolve complaints at the highest level and impose legal penalties.

Telecommunications/Cable Sector

All respondents who commented on this issue prefer the use of the Federal Court.

Financial Sector

Under the CBO industry sector regulatory model, there would be no role for either a tribunal or the courts. The CLHIA has no clear position on this issue, while CGA Ontario and ACFC support the use of the courts.

Deloitte employees support the creation of a national tribunal to back up the use of sectoral oversight bodies. They claim the Canadian courts are overburdened while decisions on privacy should be made swiftly. Canada Trust and Equifax also support the creation of a special privacy tribunal. Canada Trust says the tribunal should be composed of industry, government and public representatives similar to the Canadian Payments Association. In Equifax's view, a national appeals tribunal would deal with complaints against federally regulated industries as well as appeals from decisions made by provincial tribunals.

Commercial/Retail Organizations

The CGA does not support the creation of a tribunal. Enlogix suggests an advisory committee of private sector specialists be appointed to advise a new private sector Privacy Commissioner (who would have no coercive powers).

Information Technology Associations

CATA and ITAC support use of the Federal Court. CAIP supports a tribunal structure within the Office of the Privacy Commissioner similar to existing tribunals such as the Copyright Board, although parties should have recourse to the Federal Court of Appeal for judicial review of any legal issues. CIPS supports a similar approach but says appeals should be between the organization and the Privacy Commissioner only, so as to prevent companies from using their greater financial resources in the appeal process to prevail over individuals.

Individuals (including consultants, experts and academics)

Individual opinion is equally divided between the use of the Federal Court for appeals or the creation of a tribunal for final oversight. One suggestion was for a tribunal, with the use of the Federal Court for judicial review, where appropriate.

Highlights

There is mixed support for the use of tribunals versus the Federal Court, and little in-depth discussion of the pros and cons of either approach. The majority of business groups prefer use of the Federal Court. Privacy commissioners and consumer groups are divided on the issue. Where a tribunal is preferred, it is generally on the basis of accessibility (e.g. the courts are clogged) and, in a few suggestions, to act as a national body that could play a role in harmonizing privacy protection across all jurisdictions (as in the Human Rights Tribunal or Competition Tribunal that were mentioned by a few parties as examples of such national bodies). Where a preference for the Federal Court exists, there is also mention in submissions from some consumer groups that the legislation should not prevent individual access to lower courts, such as provincial small claims courts, to claim damages and seek awards. In one consumer group submission, there is reference to a structured approach that would facilitate such legal actions

11. What use should be made of existing industry regulators or of industry-led self-regulatory mechanisms? How can such bodies be set up to satisfy business, consumer and government expectations?

All parties generally support the concept of organizations attempting to resolve disputes directly with individuals before involving the federal Privacy Commissioner.

There is also a strongly stated position in industry groups, notably telecommunications and the financial sector, that primary reliance be placed on industry self-regulation which could include self-regulatory oversight bodies, with the Privacy Commissioner as a final means to resolve disputes in cases where no satisfactory resolution can be arrived at betwee . the parties, or when such a process is deemed likely to fail.

Within the financial sector and commercial/retail sector, many organizations also noted that they were currently subject to provincial sectoral oversight bodies, and were either subject to existing privacy protection provisions or expected such provisions to be added to sectoral oversight responsibilities.

Despite these various views, there is very little general support among respondents for the role of existing federal sector regulators such as the Canadian Radio-television and Telecommunications Commission (CRTC) or the Office of the Superintendent of Financial Institutions (OSFI). There is, rather, a strongly stated preference for ultimate oversight in the hands of the Privacy Commissioner, with assistance from federal sector regulators where required, and use of industry self-regulatory processes to the extent practical. The specific views of various parties are outlined below.

Privacy Commissioners

The federal Privacy Commissioner views his Office as the ultimate oversight agency, while working closely with existing business umbrella organizations, industry-specific associations and relevant government entities to address privacy issues through consultation, conciliation and negotiation and with the absolute minimum use of coercion and compulsion. There would be no formal role for sectoral regulators as oversight agencies.

This view is generally shared by provincial privacy commissioners who encourage sectoral bodies to take an active role in complaints resolution and development of sectoral codes.

Consumer Groups (including organized labour)

The CCC objects to the sharing of privacy oversight responsibilities with existing regulatory bodies and industry associations. CPI also believes a central body is preferable to multiple complaints-handling bodies serving specific indu y groups or sectors. FIPA, FNACQ/OC, BCCLA,and CAC also oppose sectoral regulators.

CAC Ontario and Privacy Partners state their continuing support for industry-led oversight bodies, with Privacy Commissioner oversight. PIAC warns that sectoral regulators should only be used to either refer complainants to the federal Privacy Commissioner or oversee a concurrent regulatory regime. PIAC says the government should guard against companies invoking the "regulated conduct defence" for activities specifically authorized or sanctioned by sectoral regulators.

Health Care Sector

The CDA supports sectoral self-regulation with Privacy Commissioner oversight.

Archivists/Historical/Library Associations

The OLA, which also supports binding sectoral codes where all stakeholders agree, believes sectoral oversight bodies can play a role in oversight as the first level of appeal where resolution cannot be reached between the individual and the organization.

Telecommunications/Cable Sector

Rogers and the CCTA support the continuing role of the CRTC as an oversight body. Microcell also believes the CRTC can play a continuing useful role since it has the expertise and staff to supervise the companies it regulates. AT&T and Stentor, however, believe privacy oversight should migrate from the CRTC to the Privacy Commissioner.

With regard to industry self-regulatory bodies, The AT&T Companies support continued use of an existing telecommunications ombudsman who acts on behalf of a number of companies. The Ombudsman could refer complaints to the Privacy Commissioner who would have final authority. The CWTA says it would be willing to receive, review and attempt to resolve complaints on behalf of industry members, referring them to the Privacy Commissioner where complaints could not be mutually resolved. The cable industry notes that it has an existing and well-functioning self-regulatory organization, and promotes its continued use.

Financial Sector

Many financial sector respondents are subject to industry-specific oversight bodies (e.g. insurance regulators) and have developed self-regulatory processes as well. Consequently the vast majority of responses to this question call for the maximum use of industry self regulatory processes and industry sectoral regulators.

Canada Trust, however, believes trade associations and industry ombudsmen do not have the appropriate experience to oversee privacy protection and should have no formal, legislated role in privacy protection. CGA Ontario concurs, stating that the federal Privacy Commissioner has familiarity with the issues and existing legislation and privacy protection is the central part of the Office's mandate, not just one of many issues to be dealt with.

Commercial/Retail Organizations

CGA supports the maximum use of existing processes for complaints resolution. It is CGA's view that the Privacy Commissioner should be able to delegate responsibilities to other jurisdictions and processes.

Individuals (including consultants, experts and academics)

Nine individuals commented on this question. Two do not support any role for sectoral oversight bodies. One health care practitioner suggests self-regulatory bodies with publicly appointed members could serve the public interest in overseeing professional associations. Another individual directly opposes this view, saying that appropriate sanctions could only be imposed by the State. One individual calls for sectoral oversight bodies such as the CRTC and OSFI to have the broadest array of enforcement tools as possible, including powers to act on their own volition to resolve complaints, but that the Privacy Commissioner should have final oversight authority. Another calls for such sharing of privacy protection responsibilities as long as there is a consistent approach.

With regard to industry associations, there are two comments in support of their role in public education and industry education and as industry sector "watchdogs," but no support for a formal role under legislation.

Highlights

There is clear support for the federal Privacy Commissioner having ultimate oversight responsibilities. There is very little support for federal sector regulators, such as the Canadian Radio-television and Telecommunications Commission (CRTC) or the Office of the Superintendent of Financial Institutions (OSFI), having ultimate oversight responsibilities. There is, however, some support for industry self-regulatory organizations to assist in the complaints resolution process.

12. How should responsibilities for public education be assigned?

The most commonly stated position among all respondents is that public education should be a primary and mandated responsibility of the Privacy Commissioner. Several respondents add that adequate funding must be provided for this task. The Commission d'accès, which provides public education, notes a recent proposal by a committee of the Québec National Assembly calling for public education to be mandated to the Quebec Human Rights Commission. One respondent suggests the department of Canadian Heritage and provincial educational authorities play a role in education, and a second respondent suggests Consumer and Corporate Affairs ministries could play a role in distributing information.

There is also wide recognition that public education responsibilities must be shared with business and industry, trade unions, public interest and consumer groups, industry associations and others. Many private sector organizations note the existing obligations under the CSA Standard to be open about personal information policies and practices. The federal Privacy Commissioner calls for a requirement in the legislation that organizations should make specific information available about their management of personal information and their complaints resolution policies and practices without unreasonable cost or effort. Microcell suggests that the government follow the Information Highway Advisory Council recommendations to establish a working group of government agencies and consumer groups to increase public awareness and disseminate educational materials.

The Canadian Gas Association, however, takes an opposing view. CGA state that it sees no need for further public education, since education concerning private sector use of personal information should not exceed education about public sector use of personal information.

PIAC recommends that education funding be provided from registration of data users and from financial penalties for non-compliance. However, as noted under *Question 5*, there is little general support for registration schemes.

Since the nature and extent of private sector education is left entirely to the discretion of the private sector under the CSA Standard, the Information and Privacy Commissioner for BC calls for express statutory authority for public education to be shared by the Privacy Commissioner and private sector industries. However, the Information and Privacy Commissioner of Ontario suggests such a requirement within legislation would prove to be onerous and may, therefore, be ignored by business.

The role of the media was noted by several parties, and it is suggested in one submission that consumer groups can play an effective role in educating the public if they are funded to do so, since they have a high level of public credibility. It is also suggested that the Privacy Commissioner should enter into strategic partnerships with companies and associations to carry out this responsibility.

Highlights

Most respondents agree that public education should be the primary responsibility of the federal Privacy Commissioner. It should be listed as a duty under the proposed legislation, and adequate funds should be provided for it. Organizations should have an obligation to be open to the public about their own specific information use policies and practices, as specified within the CSA Standard.

13. Should the law require privacy impact assessments of new technologies? If so, when and by whom?

Most business organizations are opposed to privacy assessments imposed by law that might threaten technology innovation, create impossible hurdles for cash-strapped small companies and drive activities and jobs to other jurisdictions.

Most, but not all, consumer groups support mandatory legislated assessments, as do one or two individuals. Among privacy commissioners, however, only the Information and Privacy Commissioner for BC supports this position.

There are also differing views on who should perform privacy assessments. CIPS, for example, believes they should be conducted or overseen by the accountable individual within the organization. Consumer groups want a process that includes public input and public approvals. Specific positions are outlined below.

Privacy Commissioners

The federal Privacy Commissioner believes the Office should provide organizations with the tools necessary to conduct privacy impact assessments on any activity or proposed activity that may impact privacy. It is unclear whether such assessments would be mandatory.

The Information and Privacy Commissioner of Alberta supports industry-developed privacy impact assessments that are submitted to the federal Privacy Commissioner on a voluntary basis for advice and direction. The Alberta Commissioner raises a number of practical concerns about a mandatory legislated approach. The Commissioner states that, if they were a legislated requirement, it would likely create an unmanageable regime. Of particular concern is the fact that many advancements in technology take place outside of Canada's borders and, due to the transnational nature of many of these technologies, there may be no practical way to curtail their use until an impact assessment is performed and approved.

The Information and Privacy Commissioner of Ontario is a strong proponent of privacy impact assessments and believes the developer of the new technology is the best party to undertake the assessment, with a supporting role played by the Privacy Commissioner. The Commission d'accès adds that companies should complete assessments on their own initiative since they must already conform to privacy legislation.

The Information and Privacy Commissioner for BC, however, maintains that privacy impact assessments should be an essential legislated prerequisite to the promotion and use of new information technologies, new products and new services that collect, use, disclose, match, link, or store personal information. Assessments should be prepared by the organization responsible for the technology, product or service, should identify competing interests to the fullest possible extent and how a balance can be achieved, and should serve as a basis for consultation with the Privacy Commissioner.

Consumer Groups (including organized labour)

CAC Ontario supports a role for the federal Privacy Commissioner to conduct privacy impacts on new technologies as soon as they appear. Privacy Partners says such assessments should be mandatory and based on an assessment procedure developed through public consultation. FNACQ/OC says companies should be required under law to inform the Privacy Commissioner of their activities and to perform impact assessments before services are marketed or, preferably, at the design stage. Public consultation should follow each assessment.

PIAC adds that assessments should be mandatory for new information technologies and should be conducted by more than one party for comparative findings, with public review and comment. The Privacy Commissioner should be able to demand further assessments if required. The legislation should also clearly define the terms "information technologies" and "privacy impact assessment."

FIPA and BCCLA, however, do not support mandatory privacy impact assessments. BCCLA suggests they would be too onerous, and it is unclear what they would comprise and what status they might have. BCCLA suggests that inclusion of a principle of justification in the legislation would achieve the same value, since it would provide citizens with a means to challenge inappropriate information use practices. FIPA states that, when new technologies or services appear that affect privacy, the cost to maintain the previous standard of privacy should not be borne by the consumer.

Health Care Sector

The CDA states that basic principles should be developed by government that can form the basis for privacy impact assessments. CIHI considers itself to be the appropriate body to carry out such assessments in the health sector.

Institutes

The U of O Centre believes the Privacy Commissioner should have powers to initiate privacy investigations, including audits and privacy impact assessments.

Archivists/Historical/Library Associations

CLARA believes the Privacy Commissioner should be able to request that organizations conduct privacy impact assessments where data matching between organizations is planned. The CLA feels such assessments are impossible to do accurately, but suggests that new technologies be required to fit the spirit of the law.

Telecommunications/Cable Sector

All respondents are opposed to mandatory privacy impact assessments, stating it is incorrect to assume that all new technologies have the potential to erode privacy. They also assert that such assessments would be too costly and too difficult to implement and would have negative effects on the competitive position of Canadian businesses. The CCTA submits that

industry must be allowed to determine, on a voluntary basis, whether or not to perform a technology impact assessment, and that market reaction is the best determinant of whether or not privacy-enhancing technologies succeed or fail.

Financial Sector

Views on this issue are mixed. Some respondents oppose legal mandatory privacy impact assessments. Deloitte employees fear that "bureaucratizing" the process through legislation could be detrimental to technological growth and innovation, stating that the marketplace can be self-governing. ICC wonders how outcomes of such assessments would be used (e.g. would companies be prohibited from using technologies or would specifications on use be drawn up?). ICC also suggests that a set of standards could be drawn up by government for companies to measure the impacts of new technologies, as an aid to compliance. CHLIA adds that companies should assess the impact of new technologies at the development stage, without commenting on whether or not this should be a mandatory requirement.

CBA believes that, rather than legislating impact assessments, consumers should be informed of any risks in using new technologies. CGA Ontario, however, believes the Privacy Commissioner should have a mandate to assess new technologies, along with the power to audit organizational information use practices.

Commercial/Retail Organizations

CGA sees no need for mandatory privacy impact assessments.

Information Technology Associations

CATA, CAIP and ITAC believe mandatory privacy impact assessments would seriously impede innovation and the speed of getting new technology to market. CATA says they would be impossible hurdles for small, cash-strapped companies and would simply drive activities, and resulting jobs, into other jurisdictions. The Advanced Card Technology Association of Canada takes no firm position, but notes it collaborated on a privacy impact assessment with the Information and Privacy Commissioner of Ontario on smart, optical and advanced cards. CIPS, on the other hand, believes privacy assessments should be performed for any new program or business function, as well as new technologies, and should be conducted or overseen by the individual accountable within the organization for compliance with the legislation.

Individuals (including consultants, experts and academics)

Individuals generally support mandatory privacy impact assessments for new or privacy invasive technologies. One individual called for their use specifically for biometric and smart card technologies and said they should be ordered by the Privacy Commissioner, who could then decide to allow or disallow the use of a new technology, or refer the decision to a privacy tribunal. Two others said such assessments should be performed by the Privacy Commissioner. Two respondents, however, believe they should be performed by business organizations, with guidance from the Privacy Commissioner, with the results either submitted to the Privacy Commissioner for review or made publicly available upon request. One individual said the

Privacy Commissioner should develop the standard for privacy assessments, but did not define who should perform them. Another called for independent assessors and public hearings, much as with environmental impact assessments.

Highlights

There are differing views on the need for mandated privacy impact assessments. Business organizations are almost unanimously opposed to mandatory assessment which, in their view, might threaten technology innovation, create impossible hurdles for cash-strapped small companies and drive activities and jobs to other jurisdictions. Consumer groups have mixed views on mandatory assessments and who should perform them, while only one privacy commissioner supports legislated privacy assessments.

It may be possible to accommodate the interests of all parties in protecting personal information while not unduly impacting the advance of new technologies and services by encouraging, rather than requiring, privacy impact assessments under legislation. Such assessments could be performed by accountable individuals within organizations and could be a consideration in any subsequent investigation by the federal Privacy Commissioner

Cooperation

14. How should responsibilities for protecting personal information in the private sector be shared among the provincial, territorial and federal governments?

Most business organizations that responded to *Question 14* believe that harmonization is important, even critical, to the success of any legislated private sector privacy regime. Reasons provided on the importance of harmonization include the potential barriers to interprovincial trade; the need for an efficient, cost-effective legislative regime; the need for a level playing field for all sectors; the negative impacts of differing privacy standards on the development and delivery of electronic commerce; and the desire to avoid the growth of data havens.

Among Privacy Commissioners, there is general agreement on the need for harmonization to ensure equity across all regions of Canada, recognizing the existing division of powers.

Dr. Lorne Taylor, Alberta's Minister for Science, Research and Information Technology, also supported the need for harmonization, as well as recognizing the need to move forward on legislation, given European developments. The Minister cautioned, however, that the impacts of legislation on trading relationships with the U.S. would have to be considered.

With regard to the timing of federal private sector privacy legislation, Stentor states that federal sector legislation should not move forward until there is a clear commitment on the part of all provinces and territories to proceed as well. Other federally regulated telecommunications carriers, notably TELUS and the AT&T Companies, also caution against the competitive inequities that would be created by federal-only legislation. The CWTA, on the other hand, sees value in a federal government initiative that could clarify the application of legislation for other levels of government. Consumer groups also strongly support federal government leadership in this area.

Among financial institutions, insurance companies and securities regulators, as well as other organizations providing financial services, harmonization is generally considered an essential element; however, there is no specific comment from federally regulated financial institutions on whether or not the federal government should proceed first. Specific comments are outlined below.

Privacy Commissioners

Most privacy commissioners support a scope for federal legislation consistent with the existing division of constitutional powers under the *Constitution Act*, 1867. The Information and Privacy Commissioner of Alberta sees value in the possibility of national, all encompassing harmonized legislation to avoid a patchwork of inconsistent, possibly contradictory laws and regulations.

The Information and Privacy Commissioner of Ontario adds that there must be a process

for resolving situations where it is not clear which level of government has jurisdiction.

Consumer Groups (including organized labour)

FIPA supports sharing of powers between federal and provincial privacy commissioners as per the existing powers under the Constitution. BCCLA and CAC Ontario say the federal government should lead with legislation, followed by the provinces. BCOAPO concurs, adding that harmonized legislation is desirable but not essential, and a federal statute, broadly harmonious with Québec's *Act*, should be put forward for other provinces to follow. BCOAPO adds that the government could assert comprehensive jurisdiction over personal information protection through its exclusive jurisdiction over telecommunications (since the telecommunications system is used to electronically amass, store and manipulate information).

PIAC also calls on use of federal powers (trade and commerce power, criminal power and general residual power) to create a national harmonized regime, saying that reliance on provincial regulation will result in a patchwork of standards and enforcement methods. PIAC adds that the federal *Contraventions Act* could be used to accommodate enforcement of legislation through provincial authorities for efficiency reasons, including resolution of civil suits through small claims court.

Health Care Sector

The CNA notes that health care is a provincial responsibility and calls for a cooperative approach that blends federal coverage with separate provincial health acts.

Government (including the European Union)

Alberta states that harmonization is vital to future privacy legislation and urges the federal government to work with the provinces before drafting final legislation. Input from the Uniform Law Conference of Canada (ULCC) should also be encouraged prior to any federal legislation being proposed.

Archivists/Historical/Library Associations

CLARA advocates one national law or harmonized provincial laws within the private sector. The OLA says federal legislation should acknowledge but supercede existing sectoral and provincial statutes.

Telecommunications/Cable Sector

All respondents cite the need for national, harmonized privacy laws between federal and provincial jurisdictions so as not to disadvantage federally regulated industries and create an uneven patchwork of laws. TELUS stresses that legislation should not impose a greater burden on federally regulated sectors than on similar sectors within provincial jurisdiction. Microcell adds that legislation must not constrain companies operating in more than one part of Canada.

Rogers and the CWTA urge the federal government to work towards a system where

there is only one set of laws to prevent multiple and potentially conflicting obligations for business. The CWTA also believes that the federal government's initiative in this area could clarify the application of legislation for other levels of government.

Stentor, however, urges the federal government not to consider legislating until the provinces have committed to moving forward with equivalent harmonized legislation.

Financial Sector

All respondents cite the need for harmonization to a common standard. Canadian Central says harmonization across the country is important to provincially regulated organizations such as credit unions.

There are differing opinions, however, on how harmonization can be achieved. In Equifax's model, a national commission within the Office of the Privacy Commissioner would have ultimate oversight, both directly over federally regulated companies, and through an appeals process, over provincial privacy tribunals. The CBO model, which has a strong component of industry self-regulation, would limit the role of the Privacy Commissioner to referring complaints to sectoral organizations and monitoring the results, thus limiting the need for any federal-provincial harmonization of legislation.

CAFII and Canada Trust say the federal government should either replace, incorporate or defer to existing statutes, including federal and provincial financial institution and insurance statutes, that create conflict and duplication.

Commercial/Retail Organizations

The Sudbury and District Chamber of Commerce states that legislation needs to be flexible, consistent, applicable and enforceable across all jurisdictions. The CGA views harmonization as essential, stating that federal law should be confined to principles and include powers to delegate federal responsibility to the provinces to avoid duplication of process.

The CDMA proposes a model similar to the *National Health Act* with the federal government enunciating basic minimum standards, but leaving specific and detailed application to the provinces.

Information Technology Associations

All technology associations believe harmonization is important. The Advanced Card Technology Association of Canada recommends a scope of legislation to match the existing powers as per the *Constitution Act, 1868* and subsequent related laws.

Individuals (including consultants, experts and academics)

All individuals who commented on this question state that harmonization is important to ensure universal privacy rights in Canada and to ensure international recognition (e.g. to meet EU Directive requirements). Respondents, as a whole, believe each jurisdiction should legislate

within their own areas of responsibility.

One individual, however, calls for a new Canadian Privacy Board to oversee privacy implementation across Canada, but with authority only to investigate and comment.

Highlights

Most parties believe that harmonization is important, even critical, to the success of any legislated private sector privacy regime and to the marketplace, yet there are few specific recommendations on how to accomplish harmonization. There are conflicting views on whether the federal government should move unilaterally on legislation ahead of the provinces.

15. What forums, in addition to those discussed in the paper, would be useful in harmonizing the protection of personal information in all jurisdictions in Canada?

The Uniform Law Conference of Canada (ULCC) is mentioned by many respondents, reflecting broad awareness of the ULCC's current project to draft a model privacy law, and support for the role such a model law could play. There is also comment that the harmonization process can be advanced through such other forums as regular meetings of privacy commissioners, First Ministers' Conferences, annual conferences of Ministers of Justice and Attorneys General, Information Highway Ministers, Provincial Chief Information Officers, the Interprovincial Committee on Internal Trade, and the Minister of Health's Advisory Council on Health Info-structure.

There are calls for active representation from business associations, trade unions, consumer groups, the health sector, the archival community, sectoral regulators and other key interested parties in whatever additional forums are developed to discuss privacy legislation at both the federal and provincial levels.

Highlights

There is strong support for the work of the Uniform Law Conference of Canada (ULCC), which is drafting a model privacy law. A variety of other forums should also be used to advance harmonization of privacy protection across all jurisdictions. All forums should involve stakeholder input to the maximum extent.

4. General Conclusions

The above short summarization and analysis of submissions cannot begin to do justice to the many thoughtful and articulate comments put forward by all parties on the issue of private sector privacy legislation. Many comments relating to the general concept of privacy in the context of our technological society could not be included, although many were deserving of mention. Other points did not relate directly to the 15 questions could also not be reflected.

The consultation process elicited 90 responses, including many comprehensive and detailed documents that reflect, in general, the interest that all Canadians attach to the importance of privacy protection and achieving the right balancing of interests.

The extent of convergence in positions and the scope for compromise suggests that a balancing of interests, reflective of the legitimate interests of all parties, may be attainable with some further effort. There is clearly agreement on the CSA Standard as a good starting point for legislation, although some further effort will be required to find the appropriate degree of precision and to consider the additional obligations suggested by some parties, as well as to consider how best to accommodate the needs of journalists, credit reporting agencies, securities regulators, medical researchers and archivists and others within the framework of a privacy law.

There is clear support for the oversight role of the federal Privacy Commissioner, the need for some proactive powers of investigation and the need for public education. There is also active support for a complaints resolution process that starts with organizations, with strong encouragement for organizations to develop individual or sectoral codes of practice for guidance purposes.

It is also clear that virtually all parties encourage the development of a national framework of harmonized privacy laws that would apply across all jurisdictions to provide all Canadians with an equivalent measure of privacy protection, and to ensure a level playing field for business. Achieving this framework should be the most important objective in advancing privacy legislation.

APPENDIX 1:

INDEX
of Submissions to the Discussion Paper

1) Summaries of Submissions from Organizations

2) Summaries of Submissions from Individuals