Data Protection in the Private Sector - Options for a Uniform Statute

1996

1996 Ottawa, ON

Civil Section Documents - Data Protection in the Private Sector: Options for a Uniform Statute

On Monday, August 12, 1996, the ULCC Civil Section approved the recommendations contained in the paper prepared by Tom McMahon and presented to the ULCC. The ULCC recommended that a uniform statute for regulating how the private sector handles personal information should be drafted and presented to the 1997 ULC conference, incorporating the recommendations of the paper presented at the 1996 conference.

The recommendations in the paper accepted at the 1996 conference were that the draft statute should:

- apply equally to all businesses and non-government organizations, regardless of the size or type of activity;
- treat all personal information the same way, regardless of the different sensitivity of some information;
- be based on established data protection principles such as those found in the Canadian Standards Association Model Code for the Protection of Personal Information;
- establish an administrative mechanism to oversee the implementation of the law (such as existing data protection commissions);
- provide the data protection commission with the power to educate the public about data protection in the private sector; investigate and mediate complaints, but only after the company complaint process has been tried first (assuming there is a company complaint process and that the process has clear and short timelines, but allow for exceptional cases where a complaint could go directly to the Commission);
- allow the Commission to publish the names of companies that do not comply with the data protection law; and
- include an offence provision for violation of the law.

More consultation should occur on the questions of:

1. how the uniform law would integrate with standards organizations that provide registration of data protection practices pursuant to the CSA Code; and
2. what is the most appropriate adjudication model (courts; ad hoc tribunals; permanent Commissioners: it may be possible for different provinces to adopt different approaches).

In addition to the recommendations in the paper presented to ULCC in 1996, the Civil Section specifically recommended that the data protection commission have the power to conduct compliance audits at its discretion on an ad hoc basis. The Committee also resolved:

"That the working group undertake to ascertain if there are effective mechanisms for the development and ratification of sectoral codes or other measures that provide more precise guidelines for the protection of privacy and disclosure interests specific to particular sectors consistent with the general principles set out in the Act."

ULCC Advisory Group on Protection of Personal Information
Tom McMahon, Chair[1]

Uniform Law Conference of Canada, August 1996

INTRODUCTION - THE CONSULTATIONS TO DATE

1. IS A LEGISLATED APPROACH DESIRABLE?

2. WHAT SHOULD THE STATEMENT OF DATA PROTECTION PRINCIPLES CONTAIN?

3. WHAT KIND OF OVERSIGHT MECHANISM SHOULD EXIST?

4. WHAT POWERS SHOULD AN OVERSIGHT BODY HAVE?
Public Education mandate
Complaint investigation powers
Complaint adjudication powers
Company complaint process first?
Technology Assessment
Compliance Audits
Remedial Powers
Order registration to the CSA Model Code?
Publish names?
Offence provision?
Damage awards?

5. WHAT SHOULD BE THE SUBJECT MATTER OF A MODEL DATA PROTECTION LAW?
Sectoral codes?

6. MISCELLANEOUS MATTERS.

ANNEX I - SUMMARY OF RECOMMENDATIONS

ANNEX II - THE PRINCIPLES IN THE CANADIAN STANDARDS ASSOCIATION MODEL CODE FOR THE PROTECTION OF PERSONAL INFORMATION

ANNEX III - SUMMARY OF THE QUEBEC MODEL

ANNEX IV - QUESTIONNAIRE

ANNEX V - PERSONS CONSULTED

INTRODUCTION

At the Uniform Law Conference in 1995, a paper on Personal Information and the Protection of Privacy was presented. The paper was prepared by Denis Kratchanov, my colleague at the federal Department of Justice, with input from a number of expert commentators. The last paragraph of Denis' paper reads:

The first step for the ULCC, if it decides to deal with this issue, is to agree on the principles that a data protection law should promote. These might be the principles identified in the CSA Draft Model Privacy Code; in any event, they should be consistent with the OECD Guidelines. The second step would be to decide on the best approach to ensure compliance with those principles, i.e. "light" or "heavy" legislation. The third and final step would be to prepare draft legislation that would be available to any government in Canada. The ULCC can play a vital role in ensuring that legislation adopted in this area by Parliament and the provinces does not lead to confusion in the marketplace for consumers and businesses alike or to the creation of new non-tariff barriers between provinces.

Earlier in the paper, the "light" and "heavy" legislative options were explained this way:

Data protection legislation can take many forms, but to be effective it needs to be based on a set of fair information practices similar to the 10 principles enunciated in the CSA Draft Model Privacy Code. The difference lies in the degrees of coercion and voluntary cooperation it relies on. A "light" version as requiring collectors and users of personal information to adopt privacy codes, based on the CSA model, within a specified time frame. An advisory body could help draft and promulgate the code, and the legislation would impose codes created by that body if the deadline had not been met. Compliance with the codes would be purely voluntary. A "heavier" version would provide a public body with the powers to force a private sector entity to comply with its own code. Between the two versions, there is a range of "medium" versions that could be adopted.

Another variation of the two options outlined above could be to design codes that are sector specific, which would allow greater flexibility to the protection of privacy interest in different contexts. Having separate data protection laws or regulations to address the concerns of specific industries such as telecommunications and insurance, might cause sever difficulties in compliance, however, since different sectors of industry exchange information and the lines between industries are beginning to blur.

After a discussion of this report, the ULC resolved:

That the Steering Committee of the Uniform Law Section create a Task Force to develop proposals for a Uniform Personal Information Protection Act which will include a statement of principles and options for implementation.

Since then, the federal government announced its response to the Information Highway Advisory Council (IHAC) report. The IHAC recommended that legislation is needed, that

there needs to be effective, independent oversight, and that all parties should follow the same rules and that the government should:

- create a level playing field for the protection of personal information on the Information Highway by developing and implementing a flexible legislative framework for both public and private sectors. Legislation would require sectors or organizations to meet the standard of the CSA model code, while allowing the flexibility to determine how they will refine their own codes. (p. 141)

The report goes on to make special mention of health records and especially the ability to identify health research participants, recognizing that obtaining individual consent is not always desirable or feasible. (p. 147) The **government response** to the IHAC report includes the following statements:

The right to privacy must be recognized in law, especially in an electronic world of private databases ... As a means of encouraging business and consumer confidence in the Information Highway, the ministers of Industry and Justice, after consultation with the provinces and other stakeholders, will bring forward proposals for a legislative framework governing the protection of personal data in the private sector.

The federal government is currently finalizing a consultation strategy and issues paper to help it develop a legislative proposal for regulating data protection in the private sector.

The reasons for legislating data protection in the private sector are numerous and were discussed in some length in Denis' paper last year. To recap in summary form, the Information Highway Advisory Council, the federal Privacy Commissioner, the B.C. and Ontario Information and Privacy Commissioners, the Canadian Direct Marketing Association, among others, have all called for such legislation. Quebec has already adopted such legislation.

In addition, the Canadian Standards Association has finalized a voluntary standard for data protection, articulating 10 basic data protection principles that should be followed by private sector organizations. This voluntary standard was unanimously accepted by a committee of government, consumer, business and other interest group representatives and demonstrates that there is a growing consensus on the need for data protection in the private sector and on the key principles that define data protection. The CSA Code became a national standard in March 1996 and is now being considered by the Committee on Consumer Policy of the International Organization for Standardization. The consultations and consensus that have already been achieved provide a good base upon which to develop a uniform statute. (**NOTE**: Annex II sets out the 10 data protection principles contained in the CSA Code and Annex III to this paper contains a two-page summary of the main provisions in the Quebec Act.)

There are important trade reasons to develop a uniform statute: to ensure that trade with the European Union countries is not disrupted by failure to meet the adequacy test of the EC Data Protection Directive; to promote a uniform approach to such legislation so that consumers and companies operating in a number of jurisdictions in Canada will not be faced

with a patchwork of differing rules; and to promote consumer confidence in electronic commerce.

The Consultations to Date

In order to advance the ULCC's resolution in favour of a uniform statute on data protection, I consulted with approximately 30 knowledgeable private sector, consumer and government representatives and other data protection experts and circulated two consultation papers asking questions on a variety of issues relating to what a Uniform statute on data protection might contain. (See Annex V for a list of the persons consulted. Not all of the 30 persons provided responses to my consultation documents.) The second consultation paper included a questionnaire (Annex IV sets out the questionnaire and contains brief "pro" and "con" statements for each question.) There were 22 responses to the questionnaire, with six from private sector interests (including two private practice lawyers), three from provincial government organizations, and thirteen responses from other sources, being Privacy, Human Rights or Law Reform Commissions, consumer or labour groups and academics.

The first consultation paper generated responses from two other private sector businesses and a meeting with the Canadian Medical Association, in addition to responses from most of the persons who responded to the questionnaire. An articling student completing his Master in Laws thesis in data protection, Tom Onyshko, wrote a lengthy letter rather than fill our the questionnaire (and is not included in the count of 22 responses to the questionnaire). Given the time-frames involved, the individuals who responded did not have an opportunity to canvass their organizations and could not express formal views of their organizations. It cannot be said that the consultations were a product of scientific sampling or that there was perfect clarity in the questions asked or responses received or unanimous agreement on any particular issue.

This paper addresses the following issues in some detail:

Is a legislated approach desirable?
What should the statement of data protection principles contain?
What kind of oversight mechanism should exist?
What powers should an oversight body have?
What should be the subject matter of a Model Data Protection Law?
Miscellaneous matters.

Given that the purpose of the Uniform Law Conference is to promote uniformity across the country, and given that Quebec has already legislated data protection in the private sector, any departure from the Quebec model would make achieving uniformity more difficult to achieve. Therefore, in the recommendations that follow, I have noted the extent to which they are compatible with the Quebec approach. At the same time, it is also desirable that regulation of data protection in the private sector be reasonably uniform with regulation of data protection for the public sector, so this should be kept in mind as another uniformity objective. That being said, John Gustavson of the Canadian Direct Marketing Association, while noting that the CDMA is supportive of some form of legislation, emphasizes his

organization's opposition to the Quebec model and argues that the Uniform Law Conference should not let the model chosen by one province dictate the uniform law the Conference might ultimately choose to adopt.

1. .Is a legislated approach desirable?

In the first consultation paper was the following sentence:

Given the report and the resolution of the Uniform Law Conference in 1995, I do not believe it would be appropriate for us to debate whether or not governments should adopt legislation or whether or not the ULC should prepare a Model Act.

Despite the above, a number of comments were received on whether or not legislation is a good idea. Many persons who responded, whether they be private individuals, or representatives of government, the Ontario Law Reform Commission, the Canadian Labour Congress or the Canadian Mental Health Association, were supportive of a legislated approach.

On the other hand, representatives of Equifax and the Canadian Bankers Association were not persuaded of the need for legislation, but accepted that if there is to be legislation, then a uniform law is the way to go. A representative of Stentor replied that framework legislation should be based on federal-provincial-territorial agreements in all jurisdictions to ensure harmonization and an equal playing field for all players in the private sector. The Canadian Direct Marketing Association (CDMA) supports the idea of "framework" legislation that relies primarily on sectoral codes for implementation. Equifax replied that it hoped that laws regulating data protection in the private sector would replace credit reporting legislation, rather than being in addition to those laws.

At the same time, no one other than the CDMA reported any difficulties created by the adoption of private sector data protection law in Quebec (although Equifax noted some consumers initially mistakenly thought the Quebec law could help them remove negative but accurate credit reports, and some data protection advocates suggested the Quebec Commission d'accès à l'information has been somewhat weak in enforcing the law with respect to the private sector). A paper prepared by lawyer Jacques St. Amant for Industry Canada quotes a speech from Étienne Dubreuil, vice-president with Teleglobe Canada Inc. as follows:

The legislation is not unreasonable; as a matter of fact, a few irritants aside, it is a statute with which enterprises will not have tremendous difficulties dealing with. If we base ourselves on the last four months experience with this legislation, Quebec firms have had to change some of their practices but most have seen this as a transparent step, satisfying both the clients and the enterprise itself. Some people would even say that it has been a good marketing tool. ... Everything considered, perhaps the only real difficulty with Bill 68 resides in the fact that it is functional approach with applicability to Quebec only. This should be less than satisfactory for Canadian financial institution enterprises which deal across Canada and for whom a multiplication of standards of protection of personal information is unacceptable.

In contrast, John Gustavson of the CDMA wrote:

[M]any participants .in the Canadian Standards Association committee that drafted the CSA Model Code for the Protection of Personal Information. _ and I would certainly include CDMA among this group _ find the Quebec law far too intrusive and an unnecessary burden on business in that province. By contrast, the great advantage of simple framework legislation, as endorsed by the government in its response to IHAC, is that it empowers industry groups, associations, and privacy advocates within individual companies to take ownership of the issue. In the process, it shifts the burden of detailed codes away from government and back on to self-regulating sectoral organizations where peer pressure and other instruments of self regulation can be utilized much more effectively. This does not necessarily mean exclusive sectoral enforcement.

Having said that, I am generally supportive of the conclusions you have drawn in response to these latest consultations. I would simply note that, although I have not had a chance to consider them in detail, there seems to be nothing in these recommendations that is inconsistent with our approach to legislation.

It should be noted that a number of Canadian companies operate successfully in other countries, such as New Zealand, which already have data protection laws for the private sector.

CONCLUSION: The responses to the first consultation paper revealed that there is a large consensus that such a law should apply to everyone in the private sector, regardless of size and including non-profit organizations, and should apply to all personal information, using standard definitions of personal information (any information about identifiable persons). The real issues will arise in the content of the law and the enforcement mechanisms and powers, and much less in whether or not there should be a law.

2. What should the statement of data protection principles contain?

The consultations did not focus very much on this question. My second consultation paper summarized responses to my first consultation paper on the question of data protection principles this way:

Most respondents agree with the CSA Model Code's statement of principles and favour a uniform law that incorporates those principles. Generally, data protection principles are fairly basic, although variations in wording can be found from the CSA Model Code, the EU Directive, the OECD Guidelines and federal and provincial public sector data protection statutes. However, the basic principles themselves do not appear to be contentious. No one recommended any other model other than legislating the CSA Model Code, except respondents from Quebec who simply noted they already have a law. **The real issue, then, is not what the principles should be but what form of compliance mechanism should exist.**

See the Annex for the CSA Model Code's statement of data protection principles.

Any statement of principles will contain ambiguities and exceptions. The CSA Model Code contains fairly extensive commentaries to explain its principles. In the May 1996 issue of *Privacy Files* (a new publication canvassing privacy issues in Canada and elsewhere), Rohan Samarajiva notes two important areas of vagueness in the Quebec Act. (His comments could also apply to other statements of data protection principles.) First, he observes that the principle which limits collection to that personal information "which is necessary" for the intended purpose of the organization. Agreeing on what is "necessary" can be difficult. Second, the Quebec Act provides that personal information is not to be communicated to a "third person" or to be "used for purposes not relevant to the object of the file." The problem here is that disclosure within a company, or to subsidiaries, may not be considered disclosure to a "third person" and it may be difficult to agree on what is "relevant to the object of the file". The CSA Model Code says that personal information shall be limited to that which is "necessary" for the purpose identified by the organization and that it will not be "disclosed for purposes other than those for which it was retained" (disclosure is defined as meaning disclosure to third parties).

Another potential interpretation problem is in the principle that knowledge and consent of individuals is required for the collection, use or disclosure of personal information, "except where inappropriate" (from the CSA Model Code). A final potential problem is that data protection principles tend not to define permissible uses of personal information _ **organizations can identify any purposes they choose.**

The first consultation paper noted a number of potential problems with respect to data protection principles, but very few of the respondents indicated concern. There seems to be agreement that

- generally worded data protection principles do provide effective data protection;
- it is reasonable to expect that requested corrections can be passed on to others to whom the original information was communicated if the time frame is short enough (e.g.: six months) and if the requirement to forward amendments is focused on information whose inaccuracy might cause harm (e.g.: it is unlikely to cause a person harm if a correction in a person's address in a direct marketing mailing list is not passed on to others who received the mailing list); and
- it is reasonable to expect that organizations can keep data segregated for specific purposes and acquired from separate purposes.

RECOMMENDATION: data protection principles are fairly universal, even though they can differ from one data protection instrument to another. The principles in the CSA Model Code represent a good base on which to build a Uniform statute and these principles are consistent with the principles in the Quebec Act which regulates data protection in the private sector. There do not appear to be significant differing options with respect to the selection of data protection principles.

3. What kind of oversight mechanism should exist?

There was a strong consensus among respondents (20/22) that data protection regulators which already exist should be the agencies that monitor the private sector's handling of

personal information, rather than using tribunals that already regulate specific sectors, rather than creating entirely new tribunals and rather than relying exclusively on the courts. Using existing data protection regulators would minimize the creation of new bureaucracies (and therefore minimize the costs associated with the legislation), would capitalize on the data protection expertise that already exists, and would promote uniformity in approach and interpretation of data protection principles for the public and private sectors.

Jacques St.-Amant, a lawyer with the Association Coopérative d'Économie Familiale du Centre de Montréal, wrote that

[I]n the context of a uniform statute which may be used by all provinces, it may be appropriate to allow for some flexibility in the area of implementation: one province might choose to grant jurisdiction on data protection to its already existing Privacy Commissioner while another might opt to grant such powers to its Human Rights Commission, for instance. ...

One thing however is clear: there is no basis for sectoral jurisdiction. Data protection principles are basically identical in all areas, territorial jurisdictions ensures more uniformity and expertise should be concentrated. That is not to say that sectoral regulators would be shut out: beyond the general principles, specific areas may occasionally require an expertise which regulators such as the CRTC may provide. By and large, however, CRTC, OSFI and others are not prepared to regulate in the data protection area, nor are they able to adjudicate in order to settle conclusively individual complaints. ...

In any event, sectoral regulation cannot be advantageous to citizens, nor to most enterprises. It would be a consumer's nightmare to face different rules and to have to find the appropriate commission depending on whether he has a problem with a bank, a telecommunication company, a utility or a retailer. It would also be a nightmare for businesses to face various regulators when trying to set their data protection policies, as the case of banks makes clear: would they be required to establish some rules in the labour regulations field, others pertaining to their consumer banking activities, and yet another set of rules applicable to their investment dealer subsidiaries?

An alternative voice was Colin McNairn, a private practice lawyer who is the author of a book on access and privacy legislation in Canada, who presented this suggestion:

I favour a sector specific approach, initially in respect of regulated industries or regulated service sectors broadly defined (e.g. financial institutions (not just banks) and medical care services (not just doctors) that are likely to be entrusted with personal information, with complaint handling through a panel of independent mediators/arbitrators assembled by the sector regulator or regulators and paid for out of levies against the regulated entities or individuals, at least where mechanisms already exist for passing on regulatory costs to such persons.

In addition, a few individuals suggested that existing information and privacy commissions and sectoral commissions could both play roles with respect to privacy. For example, Pierrôt

Péladeau, editor of *Privacy Files*, says "we need existing commissions on data protection and sectoral commissions like the CRTC to deal with the larger privacy issues than strictly data protection (ex.: telecommunication privacy, etc.)." A representative from Equifax suggested that where sectoral commissions exist, they should be used, but where one does not exist, the data protection commissions should be used. A representative from Stentor would prefer that the CRTC have a significant role in data protection issues.

Charles Ferris of the New Brunswick Human Rights Commission said that the Commission must be representative of and sensitive to the private sector environment and must carry out its functions efficiently and economically. He suggested that each sector could create a sector-specific processes which would address public education, technology impact assessments, compliance audits and complaint processes. Mr. Ferris suggested that the Model Law and the Commission should set out minimum rules for the sectors to follow, and that the Commission would supervise or "manage" the sectoral application of these rules, rather than operating the functions itself. He did not favour recognizing sectoral codes in the model law itself.

Eugene Oscapella of the federal Privacy Commissioner's Office stressed that the role should be performed by an individual Commission ***er*** rather than by a Commission.

RECOMMENDATION: Of the various options (courts only; new agencies; sectoral commissions; panels of mediators/arbitrators appointed sectorally; existing data protection commissions) there is a large consensus for using existing data protection bodies to oversee laws regulating data protection in the private sector. This is the model adopted in the Quebec legislation.

4. What powers should an oversight body have?

The most significant issues with divergent views are what powers should an oversight body have, but even here there are a number of points of reasonably strong consensus.

Public education mandate

Almost everyone agreed the Commission (whichever Commission is ultimately designated by a jurisdiction to exercise data protection functions) should have a public education power (19/22), although one respondent noted that the Commission should not bear the lion's share of this responsibility, it should be the responsibility of government. There is no express public education mandate for the Quebec Commission.

Complaint investigation powers

Almost everyone agreed the Commission should have the power to investigate complaints (18/22) and to mediate complaints (17/22). The Quebec Act provides its Commission with the power to conduct investigations.

Complaint adjudication powers

Almost everyone agreed that that Commission should be able to adjudicate complaints (nine respondents suggesting that this should be done by the Commission, seven suggesting it

should be done by adjudication panels (similar to the model of human rights commissions) (17/22). A few others suggested the better model is that of an Ombudsman, such as the role of the federal Information Commissioner and Privacy Commissioner, where the first recourse is to go to the Commissioner for mediation or a non-binding recommendation, followed by an appeal to court, which could be done by the Commissioner on behalf of the complainant if the Commissioner chose to do so.

Pierrôt Péladeau and others in Quebec find that a Commission that tries to perform too many roles can result in confusion and worse (Pierrôt Péladeau, "Visions for Privacy", *Privacy Files*, July-Aug. 1996, p. 9, reporting on a recent data protection conference in B.C.):

Nathalie Belleau, a tenant's rights advocate, and Raymond Doray, a lawyer representing large public and private data users, both faulted .the Quebec's Commission d'accès à l'information (CAI). complaint handling process because, in their opinion, it shows little respect for due process and natural justice requirements. Like many others, Doray points to structural conflicts between the CAI's many different roles: consultative body, tribunal, regulator and complaint handler. ... Two solutions were put forward: the first was to strip CAI of its judicial function and give it to an independent tribunal; the second was to set clearer and stricter practice guidelines, especially with regard to due process requirements in all the Commission's various activities.

Jacques St.-Amant's response supported the above view that adjudication should be separated from the other roles. Charles Ferris suggested that the investigation and mediation roles should be kept separate within the Commission, and that there should recourse to the Courts.

Company complaint process first?

Thirteen respondents agreed that the law should provide that individuals should use the company's complaint process before going to the Commission, so long as such a provision was carefully worded to prevent companies from using such a process to delay the complaint. It would also not apply where companies (especially small businesses) do not have a complaint process. Charles Ferris suggested there should not be a "company" complaint process procedure, but a "sectoral" complaint process that the sectors could establish. Others noted that in practice the Commission would use a "company process first" approach simply as a way to manage the volume of complaints and there is no need to put such a provision in the law. The Quebec Act does not have a "company process first" clause.

Technology assessment

Eleven respondents agreed that the Commission should play a role in assessing the data protection implications of new technologies. However, the private sector respondents did not agree that the Commission should have this power but that this function could be performed by the private sector. Two of the respondents suggested that such a role is important but does not need to be performed by a data protection commission and could be

performed by other government agencies. Eugene Oscapella suggested an appropriate government ministry could perform the role. Pierrôt Péladeau said:

We also need some kind of Office of Technology Assessment role to deal with issues beyond the strict privacy issue and provide public expertise for the conduct of public debates (this can be done through research departments of Ministries, specific agencies, funding for public research in universities, costs awards to citizens' organizations, etc.) I spontaneously tend not to give such a mandate to data protection commissioners because they tend to reduce the scope of their inquiry only to data protection related issues. ... This is a dangerous pitfall for data protection commissions: to think that data protection assessment is sufficient technology assessment. ... Technology assessment is a very good investment and does give good monetary returns (I have written a few papers on this subject). Technology assessment in fact diminishes the risks linked with systems development and diminishes the cost as well. ...

The Quebec Act does not make a specific provision for technology assessments.

Compliance audits

Only ten of the respondents and none of the private sector respondents supported the Commission performing compliance audits. Some private sector respondents preferred independent registrars. The Quebec Act does not provide for compliance audits separate from complaints but allows the Commission to make whatever inquiries it chooses on its own initiative.

Remedial powers

Order registration to the CSA Model Code?

Twelve of the respondents recommended integrating a private sector registration process into the law. Only six suggested mandatory registration of large companies ("large" might depend on the amount of personal information collected, number of employees or total revenues), and eight suggested the Commissioner should be able to order poor performers to register. A representative from Stentor suggested that registration is more effective with respect to some private businesses than others. Colin McNairn said that if governments used private standards registration processes on a wide-spread basis, this would be too expensive for the private sector. Pierrôt Péladeau stated:

Registration is needed only for intermediaries like credit bureaus with which the data subject has no direct business relationship ... This should a very light (just fill a one page form) process with no audits required. The objective is openness, public knowing of the existence of this organization.

Standard registration or certification DO NOT bring ANY benefit to data subjects. .his emphasis. The real interest is for businesses and organizations themselves: integrity of networks, business partnership, etc. No certification will prevent political conflicts with data subjects, nor can it solve them. Audits deal mostly with objective procedural requirements not with subjective conflicts. Standard registration or certification should not be mandatory

but the ordinance power .power to make remedial orders. should be broad enough to implicitly permit a Commission to ask for registration in particular ad hoc cases.

Expressing the opposite view is Colin Bennett, Associate Professor of Political Studies at the University of Victoria, who recently wrote a paper for Industry Canada in which he says "Registration to the CSA Model Code contributes a crucial mechanism for enforcement within any potential regulatory system. ... It can be used to reward good practice, and to bring the recalcitrants into line. ... The standards-registration process can relieve regulatory bodies of checking and verifying .sectoral. privacy code content." The Quebec Act does not provide for a registration process.

Publish names?

A majority of respondents agreed that the Commission should be able to publish the names of companies who were found to have breached the requirements of the law (15/22), although there was a sharp distinction between private sector and other respondents, where only two of the private sector respondents supported this idea and one of them simply noted that the publicity would be accomplished because decisions of the Commission would be public. Pierrôt Péladeau said "Publicity is the atomic bomb of a Commission, far more effective than any penalty. A Commission should always have this power." The Quebec Act provides a publication clause.

Offence provision?

Thirteen of the respondents recommended that the law should contain an offence provision, though it seems that relatively few expect an offence provision would be used often or would be very useful in promoting general compliance with the Act and satisfactory resolutions of complaints. Private sector representatives were not supportive of an offence provision. Eugene Oscapella recommended an offence provision for interference with a Commissioner's investigation, but otherwise no offence provision (similar to the federal *Privacy Act*). The Quebec Act has an offence provision for persons who collect, hold, communicate or use personal information otherwise than in accordance with the Act. Even without a specific offence, it should noted that all jurisdictions have a general offence provision where statutes do not specifically provide for an offence.

Damage awards?

Whether or not the Commission should have the power to order damage awards was not canvassed in the consultation. It would be premature to make a recommendation on this point. The Quebec Act does not expressly provide for damage awards but allows the Commission to "order the application of such remedial measures as are appropriate to ensure the protection of personal information." Tom Onyshko recommends a provision for damage awards.

RECOMMENDATIONS: Based on the above, a uniform statute should provide the data protection commission with a mandate for public education, powers to receive complaints (but generally only after the organization's process had been tried first), conduct investigations, mediation and adjudication. Whether the adjudication would be better done

by a single Commissioner, full-time hearing officers, or from an *ad hoc* roster should be the subject of further consultation. Also, the law should not expressly provide for compliance audits or for technology assessments (although it is probable and acceptable that a Commission might issue papers or reports on how certain technologies affect privacy). The law should provide the Commission with the power to publicize the names of organizations with poor performance (although even if the law did not expressly provide for this, the Commission's decisions and reports would be public in any event). It would be useful to conduct more consultation on whether and how the law might recognize to private standards registration processes. The law should contain an offence provision similar to the one in the Quebec Act.

5. What should be the subject matter of a Uniform Data Protection Act?

The consultation papers noted that there is very little uniformity in privacy matters and a wide variety of laws deal with privacy issues. The second consultation paper stated:

There is a patchwork of data protection and privacy laws already in place and adding a 'uniform' law to regulate data protection in the private sector would simply add to the heap. Almost all jurisdictions have data protection laws for their *public* sectors; most jurisdictions have separate credit reporting regulations (as noted above, Equifax is hoping a data protection for the private sector law might replace the eight separate provincial credit reporting laws); and a variety of industry and professional associations have codes which address data protection issues. Legal, medical, financial and other forms of privilege are sometimes expressly recognized in law, either in statute or common law, and constitute a form of data protection. The IHAC appears to consider medical records differently than other kinds of personal information. Ontario is apparently considering specific legislation for the protection of medical information. The protection of rape counselling records has been the subject of recent litigation and possible *Criminal Code* amendments. Many individual statutes have specific data protection rules, some of which extend to the private sector (e.g.: *Income Tax Act* and the use of the Social Insurance Number for purposes other than tax reporting; the *Bank Act* and provisions relating to security and confidentiality of financial records). The federal Privacy Commissioner has commented on the desirability of continuing public sector personal information rights for public employees who find their jobs transferred to the private sector. The CRTC has some responsibilities for privacy matters in the telecommunications industry (and it is on this basis that it has been suggested by some that the CRTC be responsible for regulating data protection in the telecommunications industry), the Office of the Superintendent of Financial Institutions has some with respect to banking.[2]

It can be difficult for the ordinary citizen to know which data protection or privacy rights apply to a given situation, how to enforce any rights they might have and difficult to understand why there are different privacy rules in different situations. These difficulties can become worse if we add to the laws that already exist sector-specific privacy codes, keep privacy torts separate from data protection remedies, keep *private* sector data protection separate from *public* sector data protection, or have multiple data protection commissions

(e.g., federal and provincial commissions with shared jurisdiction in a province, or the federal Privacy Commissioner, the CRTC, OSFI, etc., all performing data protection functions at the federal level).

Thus, **there is a considerable challenge to making laws which protect privacy uniform, understandable and accessible.** While a number of respondents are sympathetic to this challenge, there seems to be a consensus that a uniform statute on data protection stands the best chance of being accepted if it is limited to data protection matters and does not address other kinds of privacy issues and does not try to get overly specific with certain kinds of sensitive personal information.

Less than half of the respondents supported including in the model data protection law specific provisions dealing with credit reporting (although Equifax would prefer uniform provisions in all jurisdictions, preferably as part of a uniform model data protection law) (10/22), invasion of privacy torts (based on the Uniform Law Conference's model Act in this area) (7/22), workplace privacy (i.e.: limits on employer rights to keystroke, e-mail or video surveillance or drug testing, etc.) (7/22), or medical records (9/22). The general view appears to be that the data protection law should express universally applicable data protection principles that are not context or technology specific. The Quebec Act includes provisions relating to credit reporting. Most jurisdictions have credit reporting provisions in other statutes.

Tom Onyshko was one of those who favours giving stronger protections for certain kinds of personal information within the model statute.

[A] model law might include controls on the collection of at least some sensitive information. The approach of existing data protection legislation is to impose controls on the *use* of information; however, the most effective method of preventing mis-use is to the control the information that may be collected in the first place. As I wrote in the conclusion to my thesis:

For example, legislation might prohibit the collection of government identifiers such as the SIN, except where required by law. Legislation might prohibit the collection of information about key grounds included in non-discrimination sections of human rights legislation (race, political or religious beliefs, sexual orientation, etc.) unless the information was collected directly from the individual and the collection was optional. The collection of information about health or sexual habits might be prohibited outside the medical context, except where compelling circumstances required collection.

Although common sense tells us that some personal information is more sensitive than other personal information, data protection principles generally allow organizations to identify any purpose they choose and to collect any personal information that is relevant to the identified purpose. In part, this may reflect how difficult it can be to identify when personal information is sensitive and when it is not (especially with data profiling) and to know when there is a legitimate right to collect even sensitive personal information. In part, it may reflect an assumption that organizations will generally collect only information with is

directly relevant to their activities, because it would be a waste of resources to do otherwise.

Sectoral codes?

Eleven of the respondents supported sectoral codes. Some persons have the view that universally applicable data protection principles do not vary between sectors; that sectoral codes could increase complexity and lack of uniformity for data protection. Some respondents indicated that if sectoral codes were permitted, the law should shape the codes and not the other way around, and the codes should be approved by regulation. In other words, sectoral codes would be fine so long as they met the legislated standards. Whether the uniform statute should incorporate sectoral codes, and if so, how this might be done should be the subject of further consultations. The Quebec Act does not recognize sectoral codes.

RECOMMENDATION: The uniform statute should express universally applicable data protection principles and an implementation mechanism, and should not attempt to set out specific rules for medical information, credit reporting or deal with privacy issues that are broader than data protection, such as workplace surveillance and invasion of privacy torts. More consultations should be undertaken with respect to the use of sectoral codes.

6. Miscellaneous matters.

There seemed to be a general consensus that technology-specific data protection rules are not needed. The Quebec Act does not create technology-specific rules.

There seemed to be little concern among respondents about cross-border data flows or special rules for such data movements. The Quebec Act requires organizations communicating personal information from within the province to destinations outside of Quebec must take all reasonable steps to ensure that the information will not be used for purposes not relevant to the object of the file or communicated to third persons without the consent of the persons concerned (with a number of exceptions, see the Annex).

There seemed to be general level of comfort with the "opt out" for intended uses (i.e.: organizations can use personal information for identified purposes unless the individual opts out of the use, rather than requiring express consent for the use. This is particularly important for selling and sharing mailing lists). This is consistent with the Quebec Act.

Although it was accepted that it is virtually impossible to prevent persons with authorized access from using that access for unauthorized purposes, only one respondent suggested there should be a specific offence created to deal with such individuals. The Quebec Act does not deal with this problem directly.

The consultation papers did not address issues concerning the constitutional limits to what activities might be subject to federal law or provincial law. Pierrôt Péladeau noted that where there is no law, an existing law can apply. He gave as an example a company operating in a number of provinces: "Maritime workers can use the Quebec Act as their files are kept at the Montreal regional office of the company and in the Toronto head office.

Since it has a business place in Quebec, even the Toronto files are under the Commission d'accès' jurisdiction."

Eleven of the respondents suggested a uniform statute should have a provision that provides in case of conflict between applicable data protection laws, the law that best protects personal data should prevail. Others preferred to rely on the traditional federal paramountcy rule, which would promote greater certainty in the law.

Conclusion and Next Steps

In 1995, the ULCC adopted a resolution to work towards a Uniform statute regulating privacy in the private sector. Since that time, much work has been done within the ULCC context and in other contexts to find consensus among the various interested parties and much consensus has been found. The CSA Code and the Information Highway Advisory Council report are excellent examples of the consensus that is emerging. Data protection principles are fairly universal, whether expressed in the CSA Code, the Quebec Act on protection of personal information in the private sector or the European Community Directive. While the principles will be at the heart of any uniform statute, the key decisions for policy makers will be in the implementation mechanisms.

This paper has set out a number of recommendations relating to those implementation mechanisms. There are a few areas where more consultation and research may be desirable, such as with respect to the desirability or use of sectoral codes, the adjudication mechanism (panels of experts, courts, all-in-one commission), the extent of the remedial powers of a commission (damage awards, use of private registration processes, publicity?), and the relationship between federal and provincial Acts.

The task now is for the ULCC to consider the recommendations in this paper and make proposals that will advance the development of a uniform statute regulating data protection in the private sector.

RECOMMENDATION: The ULCC should approve and support the drafting of a uniform statute based on the directions and recommendations set out in this report (subject to specific changes the 1996 meeting of the ULCC might suggest), and based on further consultations and research with respect to sectoral codes, adjudication mechanism and remedial powers.

ANNEX I - Summary of Recommendations

It should be emphasized that these recommendations are the result of consultations with approximately 30 selected government, private sector and consumer representatives and other data protection experts. Not all of the 30 provided responses. There were only six private sector responses to the questionnaire (of a total of 22 responses). It cannot be said that the consultations followed a scientific sampling approach.

1. Is a legislated approach desirable?

CONCLUSION: The responses to the first consultation paper revealed that there is strong consensus that such a law should apply to everyone in the private sector, regardless of size and including non-profit organizations, and should apply to all personal information, using standard definitions of personal information (any information about identifiable persons).

2. What should the statement of data protection principles contain?

RECOMMENDATION: Data protection principles are fairly universal, even though they can differ from one data protection instrument to another. The principles in the CSA Model Code represent a good base on which to build a Uniform statute and these principles are consistent with the principles in the Quebec Act which regulates data protection in the private sector. There do not appear to be significant differing options with respect to the selection of data protection principles.

3. What kind of oversight mechanism should exist?

RECOMMENDATION: Of the various options (courts only; new agencies; sectoral commissions; panels of mediators/arbitrators appointed sectorally; existing data protection commissions) there is a large consensus for using existing data protection bodies to oversee laws regulating data protection in the private sector. This is the model adopted in the Quebec legislation.

4. What powers should an oversight body have?

RECOMMENDATIONS: Based on the above, a uniform statute should provide the data protection commission with a mandate for public education, powers to receive complaints (but generally only after the organization's process had been tried first), conduct investigations, mediation and adjudication. Whether the adjudication would be better done by a single Commissioner, full-time hearing officers, or from an *ad hoc* roster should be the subject of further consultation. Also, the law should not expressly provide for compliance audits or for technology assessments (although it is probable and acceptable that a Commission might issue papers or reports on how certain technologies affect privacy).

The law should provide the Commission with the power to publicize the names of organizations with poor performance (although even if the law did not expressly provide for this, the Commission's decisions and reports would be public in any event). It would be useful to conduct more consultation on whether and how the law might recognize to private standards registration processes. The law should contain an offence provision similar to the one in the Quebec Act.

5. What should be the subject matter of a Model Data Protection Law?

RECOMMENDATION: The Uniform statute should express universally applicable data protection principles and an implementation mechanism, and should not attempt to set out

specific rules for medical information, credit reporting or deal with privacy issues that are broader than data protection, such as workplace surveillance and invasion of privacy torts. More consultations should be undertaken with respect to the use of sectoral codes.

RECOMMENDATION: The ULCC should approve and support the drafting of a uniform statute based on the directions and recommendations set out in this report (subject to specific changes the 1996 meeting of the ULCC might suggest), and based on further consultations and research with respect to sectoral codes, adjudication mechanism, remedial powers and standards registration processes.

ANNEX II - The Principles in the Canadian Standards Association Model Code for the Protection of Personal Information [3]

Principles in Summary

Ten interrelated principles form the basis of the CSA Model Code for the Protection of Personal Information. Each principle must be read in conjunction with the accompanying commentary.

1. . Accountability

An organization is responsible for personal information under its control and shall designate an individual or individuals who are accountable for the organization's compliance with the following principles.

2. Identifying Purposes

The purposes for which personal information is collected shall be identified by the organization at or before the time the information is collected.

3. Consent

The knowledge and consent of the individual are required for the collection, use, or disclosure of personal information, except where inappropriate.

4. Limiting Collection

The collection of personal information shall be limited to that which is necessary for the purposes identified by the organization. Information shall be collected by fair and lawful means.

5. Limiting Use, Disclosure, and Retention

Personal information shall not be used or disclosed for purposes other than those for which it was collected, except with the consent of the individual or as required by law. Personal information shall be retained only as long as necessary for the fulfilment of those purposes.

6. Accuracy

Personal information shall be as accurate, complete, and up-to-date as is necessary for the purposes for which it is to be used.

7. Safeguards
Personal information shall be protected by security safeguards appropriate to the sensitivity of the information.

8. Openness
An organization shall make readily available to individuals specific information about its policies and practices relating to the management of personal information.

9. Individual Access
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 that information. An individual shall be able to challenge the accuracy and completeness of the information and have it amended as appropriate.

10. Challenging Compliance
An individual shall be able to address a challenge concerning compliance with the above principles to the designated individual or individuals accountable for the organization's compliance.

ANNEX III - Summary of the Quebec Model

This summary of the Quebec model is provided because almost none of the respondents referred to the Quebec model; a few respondents suggested it would be useful to provide more information about the Quebec model; that the Quebec law has been implemented with very little resistance from the private sector and little criticism from privacy advocates; and because any attempt to create a "uniform" approach to data protection in the private sector should give serious consideration to the only approach so far legislated.

- The principles in the Quebec Act generally reflect the principles in the CSA Model Code and the EU Data Protection Directive.
- The Act applies to all private enterprises, including non-profit organizations.
- The Act applies to all information which relates to a person and allows that person to be identified.
- Enterprises must only collect information necessary for the intended purpose, and enterprises must state the intended purposes on the file when the file about the person is created.
- Collection must be directly from the person concerned unless the person consents to indirect collection or unless the law authorizes indirect collection, collection is in interest of the person concerned and cannot be collected from the person in due time or collection from a third person is necessary to ensure accuracy of the information.
- The source of the information must be identified and included in the file when the information is collected.

- The enterprise cannot refuse to respond to a request about a good, service or job to a person who refuses to provide requested personal information unless the personal information is necessary for the conclusion or performance of a contract, collection is authorized by law or there are reasonable grounds to believe the applicant's request is not lawful.
- The enterprise must inform persons of the existence and object of the files the enterprise holds about them, of the place where the file is held and the person's rights of access and correction of the information in the file.
- Enterprises must respond within 30 days to a written request for access or correction.
- The enterprise must establish and apply security measures appropriate to the confidentiality of the information concerned.
- Information must be up-to-date and accurate at the time it is used by an enterprise.
- Personal information cannot be disclosed to third parties without the person's consent (which must be a clear, free and informed consent for specific purposes) or for a purpose specified by the Act. There are 10 purposes specified, most have to do with providing information to public bodies for various law enforcement or government program purposes, but also to debt collectors and to an enterprise's own lawyer, and to communicate a list of names, addresses or phone numbers, or any information used to establish such a list, if the communication is made pursuant to a contract with a clause prohibiting disclosure for purposes other than commercial or philanthropic prospection, gives the persons on the list a valid opportunity to refuse to be included in such a list (opt out) and the communication does not infringe the privacy of the persons on the list.
- Personal information cannot be disclosed to parties outside Quebec unless the enterprise in Quebec takes "all reasonable steps to ensure that the information will not be used for purposes not relevant to the object of the file" (or the other uses authorized by the Act, summarized above) and in the case of name and address lists, that the person has a valid opportunity to refuse to be included in such a list.
- Enterprises who refuse to provide a person with access to their personal information and enterprises who refuse to make a requested correction to personal information must state in writing the reasons for the refusal and must inform the person of the recourses available to the person. The Act provides for a number of situations where an enterprise can refuse to provide access, including for medical reasons, prevention of harm to a third party, protection of a law enforcement investigation or where providing the information would "affect judicial proceedings in which the enterprise or the requester has an interest".
- There is recourse to the Quebec Commission d'accès for any disagreement between a person and enterprise over the application of the law with respect to access to or correction of one's own personal information, or to the removal of one's name from a nominative list. The person must apply within 30 days of a denial by an enterprise. In addition, the Commission may inquire, on its own initiative or in response to a complaint, into any matter related to the protection of personal information. The Commission can order an enterprise to take appropriate steps to comply with the requirements of the Act and can publish warnings that an enterprise has not respected a Commission order. Commission decisions can be appealed, by leave, to the Court of Quebec, on questions of law or jurisdiction. There is no right of appeal beyond the judge of the Court of Quebec.
- The Act makes a number of provisions concerning credit reporting agencies ("personal information agents").

- The Act contains penal provisions for fines of $1,000 to $20,000 according to the offence. When an offence is committed by a corporation, its administrator, director or representative can be held responsible. There are offences for anyone who collects, holds, communicates or uses personal information except as provided in the Act and a separate offence for credit reporting agencies.

Note that the Act does not apply to "journalistic material collected, held, used or communicated for the purpose of informing the public"; does not provide for sectoral codes; does not require enterprises to designate a person to be responsible for its personal information holdings and practices; and does not impose record retention rules.

ANNEX IV - Questionnaire
Questionnaire on Options for a Uniform statute on
Data Protection in the Private Sector

The following questions are based on the assumption that the Uniform Law Conference will develop a uniform statute regulating protection of personal information in the private sector. It also assumes the uniform statute will adopt the principles set out in the CSA Model Code, that the uniform statute will apply to all private business within a given legislative jurisdiction, will apply to all information about identifiable individuals, and that private businesses may have their own complaint-handling processes in addition to any third party process that might be established.

If you want to expand on an answer, please provide a separate response.

Implementation Option	**Pros**	**Cons**	please check
A Commission model? Do you favour a data protection Commission of some kind with some oversight responsibilities for the uniform statute?	can provide credible, neutral, expert views; universal access to an efficient, effective complaint process	can add costs and delays, be excessively intrusive on business; fail to understand business realities	Yes No
If you do NOT favour a Commission model of some kind, would you favour: (a) complainants' recourse to civil courts only: Yes (b) regulatory offences for non-compliance and no other recourse: Yes			
If the uniform statute includes a Commission model, which Commission would it be?			
existing Information and **Privacy Commissions**;			Yes

Human Rights Commissions (or other existing agencies where such do not exist)			No
sectoral Commissions where they exist (e.g.: CRTC, OSFI, securities commissions, etc.)?	would provide one-stop regulators for business	could weaken expertise & consistency in data protection; make it more difficult for citizens to know where or how to complain; data protection might be a low priority for the sectoral regulator	Yes No
new agencies	might give more visibility to the laws	would add cost at a time of government downsizing	Yes No
If there is a Commission model, which of the following functions should a Commission perform?			
public education, data protection research, regularly published reports	promotes compliance and awareness of data protection issues.	might produce more complaints and would cost more money.	Yes No
technology impact assessments	same as above.	would cost more money and might be unnecessary. If the principles are not technology-specific, why would technology-specific assessments be necessary?	Yes No
compliance audits	can give the law more credibility, more incentive to ensure business compliance; can deal with issues that might not be	may be an indication of a presumption that business does not obey the law; would add costs; real problems will arise through	Yes No

	known to the public or that might otherwise not arise in a complaint context; can prevent problems before they arise	complaints so compliance audits are unnecessary	
primary reliance on company complaint processes? Should the law *prohibit* complaints to a third party until the company process has been completed?	company processes could provide faster, more direct responses than third party responses; companies should have the chance to set things right before third parties are called in; using the company process first would reduce the workload for other processes	might result in undue delay; might deter complainants who have no confidence in the company's process; or might mean similarly situated persons do not benefit from the complaint resolution	Yes No
registration component? If the Commission is not to perform compliance audits, would you favour a system where **(a)** the Commission is authorized to order companies who have demonstrated poor compliance to obtain third party registration; or	avoids compliance auditing costs for the public body; uses a process well-known to the private sector	registration processes are not mandatory; independent registrars are not accountable to the public; requires the existence of registrars who would provide such audits and registrations; registrars rely on continued good relations with the businesses they register so neutrality or diligence could be called into question; there is a	Yes No
(b) where companies of a certain size would be required by law to register their data		copyright issue with respect to incorporating an official Standard into legislative text; if	Yes No

protection practices with a standards registrar (e.g.: registering compliance with the CSA Model Code), presumably at the expense of the business in the usual way for standards registration		registrations are mandatory, would it be less expensive or more neutral to use government registrars rather than 3rd party registrars?; if it's mandatory, business should not have to pay	
complaint investigation	every dispute resolution function needs an investigation component	it is sufficient to rely on a mediator's role without the added cost of investigation staff; the systemic nature of the job may create incentives to find privacy problems	Yes No
mediation	the objective is to resolve disputes, not find fault, so mediation is appropriate, and can be efficient and effective	if there is an investigation or adjudication function, the neutrality of the mediation function may be called into question	Yes No
publicity. The Commission would have the power to publish the names of companies with poor data protection practices (with a right of prior notice and a right of appeal before publication)	perhaps the least expensive, more effective way to ensure compliance	may be the most intrusive of all the penalty options, with respect to its impact on the business in question	Yes No
adjudication	ensures disputes will be resolved, avoids court costs and delays, may provide more expertise and consistency and fewer	courts are adequate for adjudication (see federal Privacy Commissioner model); if there is an audit, investigation or	Yes No

	costs than a court could do	mediation function, neutrality of the adjudication function may be called into question	
Adjudication panels? If the *Commission* is not to have an adjudication function, should the function be performed by ad hoc panels of experts?	no full-time salary costs or office overhead for panel members; independent from the Commission; the model is well known in other contexts	rotating panels can reduce consistency, and can take more time than full-time hearing officers	Yes No
Offence provisions? Should the law contain offence provisions for non-compliance?	this is essential to ensure the law is respected	the federal *Access to Information Act* and *Privacy Act* do not contain offence provisions; all jurisdictions have catch-all offence provisions in their summary conviction laws	Yes No
Subject matter of the uniform statute			
Sectoral codes? Should the law give legal recognition to sectoral codes?	sectoral codes permit flexibility; recognize differences in different types of business; may encourage greater support for the law and compliance by business	a variety of codes reduces uniformity; makes it more difficult for citizens to know what provisions apply to them in different contexts	Yes No
Credit reporting laws? Should the uniform statute incorporate	would respond to a concern expressed by a credit reporting	would make the uniform statute too unwieldy to	Yes No

and replace credit reporting laws?	agency; would assist in making laws more uniform	develop and gain approval for	
"Invasion of privacy" statutes? Should the law incorporate existing statutes making invasion of privacy liable to civil action?	would assist in making laws more uniform and easier to find for the public; would build on an existing ULC uniform statute	confuses privacy with data protection; not all provinces have "invasion of privacy" laws; invasion of privacy torts include much more than private business-consumer contexts; adding this could make the uniform statute too unwieldy to develop and gain approval for	Yes No
Workplace privacy? Should the law deal specifically with issues surrounding workplace privacy?	workplace privacy is an essential aspect of data protection and privacy; such provisions would promote awareness of the issues; would create a minimum standard for workers' privacy and treat minimum privacy as a human right rather than as a "negotiable" workplace perk; would require legislators to address workplace privacy directly rather than forcing workers and business to deal with these issues on an ad hoc basis in courts and tribunals	these issues are already dealt with in collective agreements, labour codes, and by human rights laws. Another layer is not needed; adding this could make the uniform statute too unwieldy to develop and gain approval for	Yes No

Medical privacy? Should a data protection uniform statute deal with permitted uses of medical records?	this is one of the most sensitive aspects of data protection and should not be left to ad hoc treatment or identical treatment as other personal information	there should be a specific focus on medical issues. The focus is best ensured by keeping the issues separate from more general data protection principles. Any attempt to include special medical rules in the uniform statute would make the model too unwieldy to gain consensus or approval	Yes No
Disclosure rules? Should a uniform statute provide aspecific permission or duty to disclose information where it is necessary to protect the health or safety of others?	recently, Ontario doctors approved a resolution where they receive information from patients that indicate the patients are a danger to others; in the legal context, the Bernardo tapes experience shows this issue may need to be dealt with legislatively	general disclosure rules may result in too many disclosures and not enough data protection to protect a person's confidence in their doctor, lawyer, etc.; these issues are too complex for a general data protection uniform statute	Yes No
Conflicts of laws. In case of conflicts between laws in different jurisdictions (i.e.: fed/prov), should the uniform statute specify that the statute that best protects personal information shall apply?	promotes data protection; avoids the federal paramountcy rule	principle of federal paramountcy is adequate and promotes certainty of the law	Yes No

Annex V - Persons consulted

John Gregory - 416-325-7630, fax: 416-325-7135 Counsel to Cabinet Office Government of Ontario 4th floor 99 Wellesley St. W. Toronto M7A 1A1	David Phillips, Vice-President, 416-362-6092; fax 416-362-7708 General Counsel and Secretary Canadian Bankers Association Box 348 Commerce Court West, 30th floor Toronto Ontario M5L 1G2	Rosalie Daly Todd, - 238-2533; fax 563-2254 Executive Director and Legal Counsel Canadian Consumers Association 267 O = Connor, suite 307 Ottawa Ontario K2P 1P7
Robert Parent - 418-643-8782; fax: 418-643-9749 Coordinateur des lois sur l = accès et sur la protection de l = information Gouvernement du Québec 1200 route de l = Église Ste-Foy, Quebec G1V 4M1	John Gustavson, President and CEO - 416-391-2362 (ext. 228); fax 416-441-4062 Scott McClellan, Director of Communications Canadian Direct Marketing Association 1 Concorde Gate, suite 607 Don Mills, Ontario M3C 3N6	Robert McGarry - 521-3400; fax 521-4655 Canadian Labour Congress 2841 Riverside Dr. Ottawa Ontario K1V 8X7
Kerri Sinclair - 604-356-2750; fax 604-953-4348 Counsel, Legal Services Branch Ministry of Attorney General Government of B.C. 1001 Douglas St., 6th floor	Suzanne Morin, Counsel - 567-7077; fax 567-7001 Stentor Telecom Policy Inc. 45 O = Connor St., suite 1800 Ottawa Ontario K1P 1A4	John Hylton, Executive Director - 306-525-5601; fax 306-569-3788 Canadian Mental Health Association (Sask. Division) 2702 - 12th Ave. Regina Sask. S4T 1J2

Victoria B.C. V8V 1X4		
Gilbert Sharp - 416-327-8591, fax 327-8605 Director of Legal Services, Ministry of Health 80 Grosvenor, 10th floor Hepburn Block Toronto Ontario M7A 1S3	Steven Lingard, Counsel - 416-362-2031; fax 416-361-5952 Insurance Bureau of Canada 181 University Ave., 13th floor Toronto Ontario M5H 3M7	Phillippa Lawson - 562-4002, ext. 24; fax 562-0007 Public Interest Law Advocacy Centre 1 Nicholas Ottawa Ontario K1M 7B7
David Flaherty - 604-387-5629 B.C. Information and Privacy Commissioner 4*th* flr., 1675 Douglas St. Victoria, B.C., V8V 1X4	Michael Globensky - 514-493-2396; fax: 514-493-2563 Equifax Canada Inc. 7171 Jean Talon East, 6th floor Anjou, Québec H1M 3N2	Ian Lawson (Lawyer, Smithers, B.C.) - 604-847-4720; fax 604-847-1992 (formerly with the Public Interest Advocacy Centre in Ottawa)
André Ouimet - 418-528-7741; fax (418) 529-3102 Commission d'accès à l'information 888, rue Saint-Jean, bureau 420 Québec (Québec), G1R 5P1	Roland McDonald - 416-863-9600; fax 416-863-9041 Director of Security and Risk Management Mastercard International 2 First Canadian Place, suite 3680 P.O. Box 52 Toronto Ontario M5X 1B1	Colin Bennett - 604-721-7495; fax 604-721-7485 Dept. of Political Science University of Victoria P.O. Box 3050 Victoria B.C. V8W 3P5
Eugene Oscapella (CBA) - 992-4862; fax: 995-1501 Office of the Privacy Commissioner of	Judith Bedford-Jones, Counsel 731-8610 ext 2283; fax 731-1779	Tom Onyshko (CBA; - Student-at-Law) - 416-369-7200, ext. 2445; fax 416-369-7250 Smith Lyons

Canada 112 Kent St., 3rd floor Ottawa, Ontario K1A 1H3	Canadian Medical Association 1867 Alta Vista Drive Ottawa Ontario K1G 3Y6	Suite 5800, Scotia Plaza 40 King St. W. Toronto, Ontario M4Y 1R6
Charles Ferris (CBA) - 506-453-2292; fax: 506-453-2653 New Brunswick Human Rights Commission 751 Brunswick St. P.O. Box 6000 Fredricton, N.B. E3B 5H1	Carla Peppler - 905-470-8995; fax 905-470-9595 Director of Policy and Resident Care Ontario Nursing Home Association 345 Renfrew Drive, suite 202 Markham Ontario L3R 9S9	Colin McNairn (author and private practice) - 416-863-4726; fax: 416-863-4592 Fraser & Beatty 1 First Canadian Place Toronto, Ontario M5X 1B2
John McCamus - 416-736-5569; fax: 416-736-5736 Ontario Law Reform Commission	Brian Gray Senior VP of Policy and Research Canadian Federation of Independent Business - 416-222-8022; fax 416-222-7593	Jacques Dufresne (CBA and private practice) - 514-847-4475; fax: 514-286-5474 Ogilvy Renault 1981 Avenue McGill College, bureau 1100 Montréal, QC H3C 3C1
Tom Wright - 416-326-3333; fax 416-325-9195 Ontario Information and Privacy Commissioner	Ron Perozzo - 204-945-2847; fax: 204-948-2041 Associate Deputy Minister Justice Manitoba Department of Justice 7th floor Woodsworth Building 405 Broadway Winnipeg, Manitoba	Pierrôt Péladeau - 514-990-2786; fax 514-990-3085 Vice-Président Recherche et Développement, Progesta Inc. C.P. 42029 succursale Jeanne Mance Montreal Québec H2W 2T3

	R3C 3L6	
Ann Jacklin, Counsel : ph. 902-423-2633; fax: 902-423-0222 Nova Scotia Law Reform Commission 1484 Carlton St. Halifax, N.S. B3H 3B7	Marie Vallée - 514-521-6820; fax 514-521-0736; Fédération Nationale Association de Consommateurs du Québec 1215 Visitation, bureau 103 Montréal, Québec H2L 2Y7	Jacques St. Amant - 514-598-7288; fax 514-598-8511 Association Coopérative d'Économie Familiale du Centre de Montréal, 2120, Sherbrooke St. East, Rm 604, Montréal, Qc, H2K 1C3

FOOTNOTES

Footnote: 1 Tom McMahon is Counsel, Information Law and Privacy Section, Department of Justice Canada. The opinions expressed in this document are not necessarily those of the Government of Canada. The "Task Force" never met in person and its work was conducted by Tom contacting a number of government, business, consumer representatives and other experts, who then replied directly to Tom.

Footnote: 2 In addition, five provinces have 'invasion of privacy as tort' laws and the ULC adopted a model 'invasion of privacy tort' Act last year. Quebec's human rights code and Civil Code have express privacy protection and the Canadian Charter of Rights and Freedoms and the Criminal Code have provisions the implicitly create a right of privacy, for example, by creating the concepts of unreasonable search and seizure. While these laws protect "privacy" rather than simply applying to "data protection", it is clear that the two concepts are related: "data protection" protects privacy interests and privacy can be invaded as a result of poor data protection practices.

Footnote: 3 This statement of the CSA Model Code's principles is provided with the permission of the Canadian Standards Association. The material is reproduced from CSA Standard CAN/CSA-Q830-96, Model code for the Protection of Personal Information which is copyrighted by CSA, 178 Rexdale Blvd., Etobicoke, Ontario, M9W 1R3. While use of the material has been authorized, CSA shall not be responsible for the manner in which the information is presented, nor for any interpretations thereof.