

**Private / Public Sharing of Personal Information:
Lessons from the health care sector**

March 2008

**Computing in Medicine Research Group
Memorial University of Newfoundland**

Private / Public Sharing of Personal Information:
Lessons from the health care sector

March 2008

Computing in Medicine Research Group
Memorial University of Newfoundland

Edward Brown, Ph.D.
Harold Wareham, Ph.D.
Gerard Farrell, M.D.
Matthew Gillard, M.A.
Rebecca Johnston, Consultant

Questions regarding this report may be directed to:

Dr. Edward Brown
Department of Computer Science
Memorial University of Newfoundland
St. John's, NL
A1C 5S7
brown@cs.mun.ca
(709) 737-7511

Acknowledgements

This research was supported through the Contributions Program of the Office of The Privacy Commissioner of Canada.

Private / public Sharing of Personal Information: Lessons from the health care sector

Table of Contents

1	Introduction.....	1
2	Findings.....	1
2.1	Conceptual problems.....	2
2.2	Problems with defined process.....	3
2.3	Problems with process implementation.....	4
3	Suggestions.....	5
3.1	Systemic improvements.....	5
3.2	Process improvements.....	8
4	Private and Public sector legislation.....	9
4.1	Private sector personal information protection.....	10
4.2	The sphere covered by the Privacy Act.....	12
4.3	Is outsourced data under public or private legislation?.....	15
4.3.1	Differences in the public and private sphere legislation.....	15
4.3.2	Which legislation governs?.....	17
4.3.3	Who has the data.....	18
4.4	Policy and legislation.....	19
5	Lessons from the Health Care sector.....	20
5.1	Description of health care regime.....	20
5.2	Effects of the personal health information regime.....	21
5.3	Advantages of health care privacy regime.....	24
6	Technology, Standards and Innovation.....	26
6.1	The story of E-consent innovation.....	29
7	Process Model and commentary.....	33
7.1	Project inception to contract: an idealized model.....	33
7.2	Intersection of program development and outsourcing processes.....	37
7.3	Privacy in program development.....	38
7.4	Outsourcing the privacy impact assessment.....	41
8	Contractual and Outsourcing Experiences.....	42
8.1	The story of PROS.....	42
8.2	The story of “Do Not Call”.....	47
8.3	The story of the Receiver General Buy Button (RGGB).....	56
8.4	Conclusions.....	57
	Notes.....	60

1 Introduction

The mandate for this report was to examine data management by Federal agencies in the context of private and public privacy regimes, based on the insights gained through previous examination of privacy infrastructure in health care.¹ While an initial examination of the differences between the public sector and private sector legislation (the Federal Privacy Act² and PIPEDA³) was of some value, the main difficulty appeared to be identifying the appropriate locus of responsibility for procedural aspects of implementing privacy policy. However, this revealed little about the use and deployment of technology by private vendors with respect to their interaction with public privacy policy. This work therefore took on an examination of the outsourcing process for Federal agencies from project inception through to implementation. The project inception to proposal and contract award could be modeled through an examination of Federal policy documents and guidelines. However, the implementation stage of outsourcing, comprising post-contract follow-through, required examination of actual projects, not policy documents: therefore a few case studies of actual projects were undertaken to gain insight into the actual project outcomes. The results of these investigations are presented in this report.

2 Findings

What are the privacy concerns if a government agency contracts with private industry to manage personal information of Canadians? That is the question central to this report.

In many ways, the question remains unanswered. Since technology is continuously advancing, new vulnerabilities and protection schemes inevitably arise. But the issue of the “right” technology is independent of who is responsible for your privacy - a private or public entity. Technology questions exist no matter where personal information is stored. But when policy, process, and their implementation are mingled with the outsourcing of technical solutions, the interaction of these elements with privacy related technologies raises concerns, which are explored here.

The dominant finding is that the important technology characteristics (and therefore privacy outcomes) are not engaged as policy issues throughout project development. Outsourcing tends to exacerbate this situation, by leaving technology specific decisions to the

hired “experts”. We provide suggestions intended to bring policy focus to technology requirements of outsourcing.

The findings are in three categories: conceptual problems with outsourcing data management; concerns with the process as it is represented or defined in policy and legislation; and issues with the typical implementation of the process.

2.1 Conceptual problems

The privacy instruments, legislation and the oversight mechanisms all conceive of privacy in terms of data protection, and responsibilities of those who hold personal information as whether they are good stewards or custodians of that data. This precludes any broader discussion of how social interaction is changing due to modern technology and expansive conceptions of privacy: for example, collective notions of privacy, such as how government uses information for public surveillance; or allied concepts such as confidentiality, which bear a different set of moral imperatives than data stewardship. Government outsourcing, privacy and technological change all have significant interaction with social and public values. The current regime replaces all such discussion with a single criterion: are the data stewards handling the data responsibly? ⁴

This stewardship paradigm promotes other conceptual problems: for example, the case studies indicate it is still common to find privacy reduced to some form of data security, or alternatively to think of privacy as a matter of how the data is used, and security as to whether it can be accessed. In other words, even a narrow “data protection” concept of privacy, (for example, as the right to control information about yourself) is subsumed as some aspect of security. For outsourcing, this means that security (and not privacy) considerations may be what the vendor considers important.

There also can be a tendency (at least in some cases) to implicitly assume that outsourcing a project or service gives access to expert handling of privacy and security issues, along with technology expertise. In reality, the private vendor may consider such things to be policy matters. If they are not precisely expressed as part of the contract requirements, there is no reason for the outsider to assume the cost of extra privacy requirements.

There is also a pervasive assumption that statutory obligations of a government department or agency can be adequately outsourced and engaged as contractual obligations. This may ignore differences in how statute and contractual obligations function in practice, or whether the

obligations are meaningful outside the context of government administration.

The overlap in the privacy law regimes for private and public entities reinforces this ambiguity, and allow the agency to assume that the privacy obligations are taken care of by the service provider, while the service provider believes the government (as client) is the data steward and is responsible for proper oversight. Using policy instruments instead of formal legislation to protect privacy in the public sphere helps add to this ambiguity.

Despite encouraging policy statements, the importance of conducting a Privacy Impact Assessment (the main instrument for evaluating privacy impact) early in a project is simply not appreciated. It is generally treated as something that can take place at any point in the process as an “add-on”. Current procedures reinforce this attitude, by having little or no specific requirements to engage privacy considerations at particular points in a project. It is not uncommon to outsource the privacy impact assessment itself, or to include it in the data service outsourcing contract, making it the vendor’s exclusive responsibility.

Specific technology choices are not considered or deferred until very late in the process – usually close to the implementation stage, after all important policy requirements are determined. There is little to no acknowledgement that the technology choices may be the decisions that have the greatest impact on what actually happens to personal information. Policy decisions prior to implementation don’t tend speak to these choices except in generalities.⁵

2.2 Problems with defined process

Many factors discourage technology innovation. The tendency of bureaucracies and tender bidders to rely on known, proven solutions is accompanied by economic disincentives built into the contractual relationship and the nature of the market to discourage even moderate risk involved with implementing original privacy solutions. The general hidden assumption that technology vendors are privacy experts or innovators by nature is not borne out. Thus, large databases are built instead of distributed systems; data is shared instead of isolated.

Generally, projects turn to industry or vendor advice with regard to the appropriate technologies: in the case of outsourcing, this is often assumed to be part of the role of the contracted supplier. But companies responsible to shareholders are not likely to take on extra obligations unless they’re paid to do so.

While there are model contract elements available,⁶ they are vague in their terms. And

once contracts are signed, and modifications or extensions may be too costly to consider. This is late in the process to be trying to incorporate specific provision for data protection or privacy technologies.

Consideration of specific technical innovations or implications (i.e. which technologies will be used) is lacking not only because the corresponding guidance documents make limited reference to such specifics, but also because there is a lack of technical standards that relate specifically to privacy issues (as opposed to security issues). There are few resources, little information sharing, or institutional knowledge preserved between projects on which to draw. This means reliance on the service provider for such guidance is almost inevitable. Furthermore, faced with ambiguous technical standards to reference, the process may turn to security or industry standards that superficially address privacy.

Such oversight as exists in the process (specifically, the obligation to submit a Privacy Impact Assessment to the Office of the Privacy Commissioner) has no mandatory impact – any recommendations can be ignored. Furthermore, no technical audit or review is required, as part of a submitted Privacy Impact Assessment or otherwise. As a result, important choices regarding technology deployment are not encompassed by the PIA style of instrument, implying such considerations are unimportant.

2.3 Problems with process implementation

This section critiques the current implementation of the outsourcing process, based primarily on case studies.

Consistent with the findings of the OPCC's audit⁷ of a number of federal departments, it was clear that PIAs are often not conducted in any meaningful manner. The conduct of a PIA may occur late in the process, which tends to relegate it to a necessary bookkeeping exercise, rather than a careful exploration of privacy impact. This happens despite the fact the guidelines clearly anticipate PIA advice *prior* to contracting. Clearly, the lack of resources and process requirements noted above are significant factors here.

The outcomes of missing or late PIAs are predictable: lack of contractual obligations around privacy compliance and specific privacy criteria and objectives often disappear due to the focus on functionality of the project. This is despite that fact that attention to these elements of the contract do appear (at least in some vague form) in the guidelines.

In some cases, even pro-forma adherence to the PIAs or reviews is lacking. For example, low-cost preliminary PIAs can be conducted which may avoid the expense and effort of a full Assessment. This also should encourage early consideration of privacy issues. But these effects simply aren't prevalent in practice.

The assessment guideline documents⁸ are reported to be difficult for even experienced privacy experts to navigate. Possible causes are vagueness and a lack of focus on practical outcomes, such as specific guidelines related to technology choices or deployment. This encourages a disengaged, "check the box" attitude toward guideline compliance.

The privacy community has come to recognize several categories of assessment; using terms like conceptual PIA (based on early and general project scoping), design level PIA (which would look at data flows and interaction), technical PIA (focused on the technology elements) and implementation PIA (examining the system as actually constructed). However, the multiple roles and need for ongoing assessment is not recognized in the outsourcing process; failure to adopt such terminology disguises the limited scope of the PIA actually conducted.

Typically, there is no ongoing oversight requirements with respect to privacy built into outsourcing contracts. Therefore, the idea that there could be a cost to maintaining or updating technology or that privacy assessment and oversight should be an ongoing commitment is lost, with the ultimate result that unplanned fixes at a later time at greater cost.

With little centralized resourcing for privacy assessment, the opportunity for capacity building is missed. Therefore any expertise of experience built is likely to be lost or isolated to contractors or within specific departments.

3 Suggestions

The following suggestions are attempts to adjust the policy scope of outsourcing projects to consider technology implications for privacy early and throughout the development of an initiative.

3.1 Systemic improvements

There is a need for a broader discussion that looks past the data stewardship paradigm to the impact of specific information technology advances and government outsourcing on social and cultural values related to privacy. This would include problems of public interest such as the

appropriate role of public and private entities, government surveillance and national security. Such a discussion should promote collaborative research and development. It should inject consideration of basic rights and the proper role of government and industry in protecting individuals into the policy overview of government projects.

Broader themes or debate over social values should not be lost in the discussion of specific outsourcing projects merely because the mandate of institutions such as the Office of the Privacy Commissioner may not encompass them. While such an initiative might be supported by industry and speak to e-government and related public initiatives, it should not be dominated by institutional or by industry interests. To be meaningful, this has to engage public participation and debate, and not merely conventional “stakeholders”.

The differences between the public sphere and private sphere privacy protection are relatively minor compared to non-compliance issues, but harmonization would certainly be beneficial. Certainly some recognition is needed that policy instruments are being used in the public sector to enforce privacy protection that is legislated in the private sphere. More importantly, tools are needed (which might be incorporated into PIAs) to address the different views of responsibility that the federal agency and the service provider may adopt. This can be in the form of detailing how each data protection obligation under the adopted privacy model (primarily the CSA code plus requirements in the Privacy Act) is being fulfilled. At present, it is sufficient for departments to merely contend they are (or will be) fulfilled.

There is no question that privacy concerns can be properly accounted for in service delivery with an inter-departmental context.⁹ But there is a need for a common government resource on privacy technology distinct from the Office of the Privacy Commissioner. Expertise that could be invoked on any departmental initiative would help eliminate superficial conceptual problems (such as conflating privacy and security measures), technical inadequacies, and process flaws.

A central resource should also develop and/or promulgate technical and process tools that are presently lacking and provide a locus for capacity growth, to capture and reuse process and technical skills and knowledge between privacy related projects.

Among the technical tools and skills that would be beneficial:

- reference architectures, testing and evaluation suites for privacy related technologies
- a catalogue of privacy technical solutions with an evaluation of their effectiveness
- objective privacy evaluation tools for industry

- requirements and arrangement (how to conduct) of privacy technical audits for (or on) outside agencies
- assessment of current industry solutions to determine strength (and other aspects) of privacy protection

And related process tools and skills:

- guidance documents, best practices and project experience skills related to privacy assessment
- a master project development guide that untangles the various sources of outsourcing, contract, and privacy requirements
- guidelines for engaging consultants to conduct assessments
- a management framework to assist departments review work when the PIA is itself outsourced, so the findings are integrated back into the project development process.
- training for project staff, consultants, and contractors related to privacy assessment, process and technical knowledge
- A pre-screened list of external experts that could be consulted.¹⁰

An internal centre of expertise available to departments and agencies to obtain information and services on technology decisions would improve government personnel's ability to interact with industry in an informed manner. Such resources are valuable either to evaluate outsourcing proposals or internal projects on a technical level.

As part of this resourcing, the government of Canada could drive innovative solutions through the encouraging of privacy technology research through agencies such as Industry Canada. IT projects could also become a venue to showcase results to the broader communities with demonstration initiatives. A common test facility for industry, academics and government to meet to examine existing solutions is worth consideration.

A general recognition of the industrial, economic, policy and bureaucratic barriers to innovation, particularly in terms of technology innovation, should be built into outsourcing activity. One possible approach is to add specific recognition of innovation opportunities (as decision points) in the outsourcing process. The choice to innovate or not should be explicit, along with the criteria used. Some of these opportunities are easy to recognize (any time the vendor says "that's not the way it's done!" is a probable clue.)

Innovation barriers are particularly important because of legacy problems that are inherent in software systems. Since a technical solution may quickly become outdated, continuous review and update of technical solutions need to be recognized as part of the cost of outsourcing.

3.2 Process improvements

A clear statement of how privacy obligations (under the policy guidelines and the Privacy Act) are divided between the service provider and the federal department after the contract is in place should be part of the SOW/RFP process. Many pertinent elements appear in the guidance documents, generally requiring confirmation they are addressed, but without specificity as to *how* they are addressed. This will do more for ensuring the complete panoply of protections are in place than efforts to harmonize public and private privacy legislation. The outsourcing process needs a detailed model framework that specifies timelines and delivery points for assessments and reviews. Significant consequence for an inadequate privacy assessment or poor review rating must be built into the privacy assessment process for it to be taken seriously. This has to include a decision point on halting the project based on inadequate privacy protection.

In addition to technology assessment tools and centralized expertise suggested above, details of technology elements need to be considered during a Privacy Impact Assessment. The vague conventional language and adjectives distinguishing “conceptual”, “implementation” and “technical” variations of PIAs need clear distinction with references to specific technologies and issues to be addressed. This will compel specific technology assessments. Currently, the PIAs can be conducted largely with respect as a business process or quality control analysis, with little critique of specific technology solutions. The development of a tool that specifically analyzes technical implementations being proposed would help guide technology decision makers and shape architectural decisions, whether it was employed in-house or outsourced. It could also help discourage the bias that “conceptual” elements of a program are “preliminary”, and therefore the technical elements do not appear in preliminary or pre-contract stages. Similar efforts have been proposed to integrate PIAs with Technical Risk Assessment instruments (TRAs) or regulatory compliance tools¹¹

The language of privacy policy needs to incorporate terminology that is technologically meaningful. While the current structure of PIAs around fair information practices (access, consent, safeguards, and so on) is important, terms like “data minimization” and “linkability” which describe privacy-related characteristics of the technology are less prominent. However, such language represents the necessary bridge between technology solutions (authentication, trust management, and so on) and policy values. A lexicon is needed that can be used not only in

policy instruments but also in technology tools such as the reference architecture suggested earlier. In combination with clarification of different PIA types, this should help address the reputed difficulty in understanding and applying PIA guidance documents.

As part of a central resource base, additional model clauses for outsourcing contracts are needed that reflect specific privacy concerns.¹² There is anecdotal evidence that contracts often don't articulate even the privacy and security features specified in the PIA guidelines, let alone refer to specific technology solutions or evaluation criteria.

The following steps should be included (and formally noted) prior to the contracting stage, and considered for inclusion in the contract if they are not addressed elsewhere. In some cases, they should be included in SOW/RFP:¹³

- Completion and successful external review of a preliminary or conceptual PIA prior to contracting
- Conduct of a (possibly second) PIA or similar instrument that includes technical elements and technology decisions of the project.
- Identification of technology choices that have completed and those that are outsourced, including recognition of architectural requirements
- Identification of how the privacy knowledge and expertise developed will be captured by government for future use.
- Identification of the specific privacy technical standards and evaluation process, including reference architectures or tools that will be used by the contractor and to evaluate the contractor's product or service.
- Identification of how responsibility for specific privacy obligations (under the Privacy Act, federal policies and fair information practices) will be distributed between the government agency and the contractor.
- Identification of which security and privacy concerns will be addressed by technology; which are created by technology; and which need to be addressed through policy development and training.
- Identification of the any technical capacity or privacy issue that motivates outsourcing.
- Analysis of current state of the art and opportunities to innovate in terms of privacy protection
- Provision for ongoing/cyclical application of privacy assessment and review of aging technology, possibly as an audit process.

4 Private and Public sector legislation

In this section, some of the legislation that defines the private and public spheres' privacy protection regime is examined. The ultimate conclusion is that there are some issues that deserve attention, but most of the discontinuity between spheres is obviated by the development of

federal policy in the area. The major concern in terms of individual protection is the ambiguity surrounding *where* responsibility for stewardship of data lies: to what extent does it remain with the government agency, and to what extent does it “follow the data” to be managed by the private vendor.

4.1 Private sector personal information protection

The Federal *Personal Information Protection and Electronic Documents Act* (PIPEDA) governs the use of personal information in the hands of organizations operating in the private commercial sector, except in provinces with legislation that has been declared substantially similar to the PIPEDA. Currently, three provinces – Alberta, British Columbia and Quebec – have such privacy legislation displacing PIPEDA for private vendors under provincial jurisdiction.¹⁴ The federal, Alberta and British Columbia private-sector laws all share the same theme: governing collection, use and disclosure of personal information by private sector organizations.¹⁵ It is possible that multiple jurisdictions will be relevant in a federal project where provincial agencies are involved. The PROS case study¹⁶ encounters this exact scenario. In that situation, a comparison of different jurisdictions’ privacy laws in the context of the specific initiative is unavoidable. However, more typically data management outsourced by a federal agency would be considered a Federal work or undertaking subject to federal statute.

PIPEDA incorporates the CSA Model Code Principles as its Schedule 1. The code lays out ten principles for organizations to follow in handling of personal information. They read:

- 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 when 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 the law. Personal information shall be retained only as long as necessary for 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 for the organization's compliance.

A rather unusual piece of legislation, the Schedule also has extensive commentary (as numbered sub-principles) on how the principles might/should be interpreted, making compliance something of a matter of understanding the privacy culture in which the legislation operates. Sections 2-10 of PIPEDA provide some legislative guidance to interpreting the operation of the Act, laying out exceptions to the consent requirement for certain collection, uses and disclosure (s. 7) such as law enforcement, investigation, scholarly work, journalism; has sections indication how provision of access works (s.8-10); a complaints process that engages the Federal Privacy Commissioner (s.11) with powers to investigate the complaint (s. 12) and make recommendations (s.13). There are no enforcement powers invested in the Commissioner by the Act, but action can be taken in Federal Court (s. 14-17) if a Commissioner's report or the organization's response is not satisfactory. The Commissioner also has broad powers to undertake a compliance audit of an organization (s. 18-19).

The Privacy Commissioner also offers a great deal of assistance with tools and advice so organizations can undertake to ensure compliance with the Act, including compliance guides available on the Commissioner's website.¹⁷ The use of Privacy Impact Assessments – generally a complex and detailed evaluation process - can be mandated for public sector organizations, but as yet is not imposed or recommended for private businesses; presumably because the requisite

overhead for conducting a large scale investigation would be prohibitive for many small businesses. Indeed, even in the public sector a “Preliminary PIA” may reveal that the expense of conducting a full PIA is unnecessary if privacy concerns do not arise.

The two key notions of PIPEDA are “reasonableness” and “consent”. For reasonableness, Section 5(3) of the Act specifically provides that personal information only be collected, used and disclosed for purposes that a reasonable person would consider appropriate in the circumstances. This standard is applied regardless of whether consent has been given for the collection, use or disclosure. As for consent, the general rule is that personal information can only be collected, used or disclosed with the knowledge and consent of the individual unless an exception applies or the information is excluded from the Act.¹⁸

4.2 The sphere covered by the Privacy Act

The federal Privacy Act¹⁹ applies to federal agencies – in fact, the same agencies are specifically excluded from the operation of PIPEDA because of the Privacy Act.²⁰ The Privacy Act has been in operation for longer than the PIPEDA, and has as its mandate to extend the laws of Canada that “protect the privacy of individuals about themselves held by a government institution and that provide individuals with a right of access to that information”. (s. 2) As such, the provisions behind the Privacy Act can be seen as a progenitor of the PIPEDA, and many similarities can be noted.

The Privacy Act has a particularized definition of personal information as information “recorded in any form including...” information relating to race, national or ethnic origin, colour, religion, age or marital status; information relating to medical, criminal, or employment history; financial transactions; identifying numbers, symbols, “or other particular assigned to the individual”; “address, fingerprints, or blood type; personal opinions or views; correspondence sent to a government institution that is of a private nature; the name of the individual where it appears with other personal information or where disclosure of the name itself would reveal private information” and exempts information that relates to positions or functions of a government employee; information about individuals who are or were performing services under contract for the government; information relating to discretionary benefits of a financial nature; information about an individual who has been dead for more than 20 years. (s.2). The PIPEDA merely

indicates more broadly that personal information is information about an identifiable individual, although it incorporates some of these exceptions in specific consent or access provisions.²¹

While there is no endorsement of a canon of privacy principles in the Privacy Act, implicitly it incorporates notional “fair information practices”, a term often used to refer to the CSA code principles, or sometimes to alternative concepts (for example, a different list might be protection, accountability, consent, transparency and control). Perusal of the Privacy Act shows many of the same obligations familiar from the PIPEDA, recited in specific sections of the Privacy Act. However, it also shows a public policy nuance in language like “transparency” (instead of “openness”).

Under the Privacy Act, personal information can only be collected by a government institution when it relates directly to an operating program or activity of that institution (s.4); personal information under the control of government may only be used and disclosed under certain conditions, primarily for the purposes of an appropriately authorized program. (s. 7, 8, 19-28).²² This is reiterated in the *Privacy Impact Assessment Policy* (the policy that mandates the use of PIAs when establishing federal programs) – it states that federal and provincial privacy protection documents “are premised on the fundamental concept that individuals have a right, subject to the explicit provisions of other legislation, to control the collection, use, and disclosure of their personal information.”²³ The crucial distinction from the private sphere legislation is that rather than a list of exceptions to the requirement for consent that are based external overriding purposes (such as law enforcement), the intended purpose (the legislated use) of the information is the justification for collecting information regardless of consent. For a private business operating under the PIPEDA, this is *exactly* when consent would be required.

The access principle also appears in the Privacy Act in similar terms to PIPEDA’s section 9. Every Canadian citizen or permanent resident “has a right to and shall, on request, be given access to (a) any personal information about the individual contained in a personal information bank; and (b) any other personal information about the individual under the control of a government institution with respect to which the individual is able to provide sufficiently specific information on the location of the information as to render it reasonably retrievable by the government institution” (s 12(1)); every individual who is given access to their personal

information can request a correction or notation to the information (s 12(2)); an individual can make a request for access to personal information to a government institution (s 13(1)); the government institution must respond to the request for information within 30 days (s 14); the 30 day limit can be extended under certain conditions (s 15); if access is granted, the government institution must give the applying individual the requested information (s 14(2)); if access is refused, the government institution must state that the personal information does not exist or specify the provision of the Privacy Act upon which the refusal is based (s 16 (1)).

The complaints provision (to ask the Privacy Commissioner to examine the conduct of a federal agency) is also similar to PIPEDA provisions: the Commissioner shall receive and investigate complaints from individuals or initiate complaints (s. 29, 34); any individual who has been refused access to personal information and made a complaint to the Privacy Commissioner may appeal to the Federal Court to review the matter following the completion of the Privacy Commissioner's investigation (s. 41).

Notification provisions are somewhat different between public and private spheres: a government institution shall tell any individual from whom personal information is being collected about the purpose for which information is being collected (s. 5(2)); and a government institution shall record use of personal information (s 9). In PIPEDA, notification under s.9 is generally required for the disclosure of personal information when consent is not given (i.e. when an exception to consent is used to justify the disclosure). Since in most other cases in the private sector, consent is required (and consent to particular uses of personal information) the effect is similar: you would probably not need notification of disclosure to which you consent. The distinction is an aspect of a public body's statutory authority to deal with personal information without consent.

Both the PIPEDA's Schedule (4.7.2) and the Privacy Act s. 6(3) include provision for destruction of personal information when it is no longer needed.

One clear difference in the Privacy is the provision for Personal Information Banks – a construct that is not defined, but logically houses “all personal information under the control of the government institution...” (s.10) which is administrative in nature or accessed by a personal identifier of some kind. The implicit idea is to be able to track what information the institution has on individuals so it can be reviewed for appropriate utilization (s. 71(3-4)). An index of

these banks is published under s.11, so that it is public knowledge what information the government is holding (although not the information itself). There is no requirement that the Personal Information Bank be a physical aggregate, such as a central database, although the wording might suggest that is the most practical way to comply with the requirement – and one would expect a tendency to aggregate data in this fashion.

4.3 Is outsourced data under public or private legislation?

4.3.1 Differences in the public and private sphere legislation

One of the jurisdictional problems that arise is whether the outsourced data is covered by the public or private legislation. This would have implications both for the rules that apply, and which parties are responsible for fulfilling any obligations.

In very broad terms, the answer to this question may be moot. As indicated above, the same themes and general types of protection for individuals that are outlined under PIPEDA also appear in the Privacy Act. Furthermore, if the data services are outsourced to a private company, one would expect the Federal agency to impose the same obligations on the service provider, either in the form of contract or statutory provisions.

However, there are some differences in the legislative regimes. The Privacy Act includes PIBs (Personal Information Banks) and specifically endorses the exploration of efficiencies and improved services by exploiting such PIBs (s. 71). No such mandate to use the collected information for the public good exists in the private sector legislation.

The Privacy Act does not explicitly include the CSA fair information principles and the detailed suggestions accompanying them in the PIPEDA Schedule. While many of these details are themselves general in character or seem to be obvious extensions of principles (e.g. 4.10.4 indicates an organization shall investigate complaints it receives and amend its practices as necessary), others provide clear additions to the basic principles.

For example, the “safeguards” principle under the Schedule is elaborated to require separate consideration of physical, organizational and technological measures.²⁴ This would certainly prevent a narrow interpretation of the duty to protect personal information that might survive scrutiny under the Privacy Act. Education and training is also prescribed for employees or staff that deal with personal information, an activity that would not necessarily be considered

as a “safeguard” measure without such specification.

Although the public sector organizations may appear less scrutinized or regulated than the private sector, a significant factor in these discrepancies is the age of the Privacy Act. As it predates the PIPEDA and the development of the CSA model code for handling personal information, one would expect the PIPEDA would update and expand the principles inherent in the Privacy Act, and not necessarily the other way around. Therefore it is not surprising to find “gaps” in the Privacy Act with respect to a more recent statute, nor that principles are recited and organized in a somewhat different manner. Furthermore, the federal government has other policy instruments that can be used to update its practices without the intervention of parliament through legislation.

The Privacy impact assessment policy and its associated guidelines are perhaps the most pertinent of these instruments.²⁵ These guidelines indicate an assessment is to be conducted for new or modified program that affect personal information, and provides the basic organization of such an assessment. These guidelines reveal a structure oriented to the CSA model code, breaking down the assessment process in an instrument with components that mirror the ten principles of the PIPEDA schedule.

In other words, government policy documents indicate an acute awareness and intent to implement fair information practices, at least at the supra-departmental level, whether or not a specific mandate for them appears in the Privacy Act or other pieces of legislation. In fact, these guidelines established by the Treasury Board Secretariat for the public sector may be used by private industry – nominally governed by the PIPEDA – to interpret their obligations under fair information principles.

While the lack of detailed legislative guidelines for fair information practices is mediated by comprehensive policies, there is a nominal concern of whether policy as a subordinate form of legislation will carry the same impetus for implementation that a clear legislative mandate would provide.

The most significant practical difference between the private and public spheres appears to be the broad authority of Federal agencies to collect information without explicit consent, in contrast to the private sector organizations that are far more restricted to gathering consent for the uses to which they apply the collected information.

4.3.2 Which legislation governs?

There is a significant question of which legislation governs the control of personal information when a private vendor is managing the data for the government agency. Arguably, the private sector legislation may still apply to the private sector entity, and the public sector legislation to the government entity.

That is the implicit position reflected in the Treasury Board Secretariat's guidance document "Taking Privacy into Account Before Making Contracting Decisions:"²⁶ (p. 12):

In addition, the government has a duty to include other specific privacy protection provisions in the contractual agreement to ensure that the contracting out of government programs and services does not result in a reduction of privacy protection. There may be instances where federal institutions subject to the Privacy Act enter into contractual agreements with organizations in the private sector that are subject to other legislative privacy requirements at the provincial or federal level, such as PIPEDA. Federal institutions faced with this kind of scenario should, in consultation with their institution's legal and privacy officials, conduct a thorough legislative and policy analysis of the requirements of both laws and develop contractual clauses in keeping with the more stringent privacy principles or standards of the two laws.

However, this interpretation can be problematic for a private vendor, which may see capacity for a federal agency under the Privacy Act to collect personal information without consent (for a government program) as necessary for their (the private vendor's) operation of the government program or service. The vendor, after all, will not be obtaining consent for the collection of personal information (as would be required if the private sector legislation applied).²⁷

This could be a greater concern if the private vendor takes the position that compliance with privacy protection requirements is exclusively an issue for the federal agency to observe under the Privacy Act. For example, provision of access to the data and complaints might be difficult for the federal institution without mechanisms put in place by the private vendor. The federal agency would presumably enforce its obligations by ensuring the mechanisms are in place through its contract.

The TBS guidance document²⁸ does in fact provide for a check that such provisions are in place in an outsourcing contract (Appendix B). However, this can raise the opposite concern: will contractual obligations including privacy obligations be an adequate substitute for oversight by a Federal agency? In other words, there is little impetus for a federal institution to maintain

the cost and overhead of compliance with privacy information protection if they outsource the data management, and believe they have engaged (and paid for) security and privacy expertise to accompany the program implementation.

The Public Works department (PWGSC) provides standard contract language²⁹ for the use of government departments, which does require the contractor to acknowledge the existence of the Privacy Act. These terms are directed at conventional contracts that might disclose personal information, not for the large scale management of personal information databases, and therefore provide little assistance with such outsourcing. A report from Alberta's Privacy Commissioner's office has more suggestions³⁰ including cyclical audits, security and confidentiality clauses, liability for breaches, return and destruction of information and injunctive relief; and the federal guidance document on privacy in contracting decisions³¹ has a similar checklist in its appendices.

4.3.3 Who has the data

Both the Alberta report and the Federal guide to contracting decisions are largely concerned with the exposure of Canadian personal information to disclosure under the US PATRIOT Act, should Canadian personal information end up stored or processed in the US. In response to this concern, both documents insist on scrutiny of the laws in any extra-territorial jurisdiction in which the data or the contractor will reside to assess the risk of exposure. Drawing up short of precluding such outsourcing entirely, the federal document notes the tension between risk of exposure of data to foreign governments and market access guaranteed by international trade agreements. The Alberta report further speculates that outsourcing the data management may also bear higher risk to *inadvertent* exposure to the US (as well as to malware and other intrusions or misappropriation of data). But currently there is no general approach to legislating *where* the data actually resides.

The data residency issue is one in which is at least partly driven by public concern over the exposure of data. This is subtler than simple risk assessment: public values are connected to the act of outsourcing,³² and more particularly when privacy is involved. These values, and not just the effectiveness of solutions, should play a role in policy determination.

One way to probe the public values associated with contracting out is to ask if statutory obligations of a federal agency can be adequately substituted by contractual obligations of the vendor. As an example, consider the suggestion that the vendor indemnify the government for

breaches of its obligations under the contract.³³ This is a fairly standard contract clause, but it is difficult to anticipate its application if privacy principles are not honoured. For example, if there are inadequate access provisions or complaints process, a pecuniary remedy is of no benefit to the agency or the private individual whose information is compromised – the process needs correction. Often, under the complaints provisions of the legislation, there are no pecuniary damages – there is only the Privacy Commissioner’s recommendations. And some compliance issues are not even visible (how do you tell if a private vendor has destroyed or deleted all copies of information as required once it is no longer needed?)

On one level, this is a matter of legal force: statutory compliance can have a different impact than contract. The decision to honour or breach a contract provision by a private company is an economic one. In contrast, the only remedy for statutory noncompliance is to comply. In the case of a statutory compliance issue under the Privacy Act, an individual can pursue the government agency, which would in turn have to pursue the private vendor under contract.

The worst possible scenario is when neither party is engaging its obligations: that is, where the vendor believes privacy is the purview of the federal institution, and the federal agency believes privacy protection has been engaged as part of the data service solution.

4.4 Policy and legislation

Do the differences between private and public sector legislation create privacy concerns in the context of outsourcing data management? There is no doubt that the Privacy Act shows its age when compared to the private sector legislation, but these differences fade when the entire federal privacy policy regime respecting fair information practices that has developed more recently is considered. More problematic is the ambiguities that remain due to the overlap between private and public sectors, which do not yield clear answers as to where responsibilities lie and how compliance and performance is to be assessed and enforced. Revisions to harmonize the public and private sector laws would not be very beneficial primarily unless it took on these problems.

Data protection legislation has been harmonized for the health care sector in several jurisdictions. The report turns to those experiences next.

5 Lessons from the Health Care sector

5.1 *Description of health care regime*

Primarily due to the initiative of Health Infoway,³⁴ the electronic infrastructure for Electronic Medical Records is one of the most advanced efforts in terms of integrating privacy and security concerns with technology in personal information. Additionally, health care provides an interesting foil because the nature of the personal information is highly sensitive, in many cases the most private information that an individual may possess.

The related infrastructure has advanced on both policy/legislative and technology fronts since the inception of efforts for pan-Canadian interoperability in EMRs, which is the mandate of Health Canada Infoway. Four jurisdictions have adopted health information specific legislation³⁵ and Infoway has (in co-operation with provincial, federal and industry) developed a blueprint for systems architecture, including a security and privacy framework.³⁶ The interest in these components led to our research team³⁷ to conduct an examination of the interaction of privacy technologies with the legislative and health care regimes. Many of the observations in this section draw on the lessons learned during that effort, and provide some grounding for the issues that arise in the remainder of this report.

One of the similarities with the focus of this report is that health care operates in both private and public sectors: a physician working in a private clinic usually will have hospital rights in a quasi-governmental facility. In the clinic, the physician is in a private organization: crossing the threshold into the hospital, his work may become subject to public sector control. This could be the case even if the physician is performing the very same task with the very same personal information in two different locales.

Four jurisdictions have resolved the public/private dichotomy with specific legislation that provides uniform treatment for personal health information in both spheres. Other jurisdictions appear to be moving in the same direction, with their own health information legislation. The general thrust has been harmonizing the treatment of health care information (including personal information) not only between public and private sectors, but also among provincial jurisdictions. Although many differences in treatment of specific rights remain between provinces (for example, the scope of patient consent has some variation), many common themes have arisen.

One important construct is the notion of a Health Information “custodian”³⁸ This is a category of person (or organization) entrusted with an individual’s personal health information. The requirements for specific consent and oversight are somewhat relaxed when a custodian shares information with another custodian, thus facilitating the movement of information among a patient’s “team” of care-givers³⁹ (e.g. lab technicians, specialists, pharmacists, and so on). The interpretation of complex and overlapping legislation governing disclosure and collection of information is replaced with specific statutory requirements for appropriate controls and safeguards between and among custodians sharing health information (which will in some circumstances still entail patient consent.)

5.2 Effects of the personal health information regime

One concern that arises about the privacy legislation in general is whether the emphasis on data protection is a good characterization of privacy, in terms of protecting individuals. There are many aspects of privacy, including how personal information is characterized publicly, the choice not to participate in government sponsored programs, choices about how to interact socially with others, which are not specifically part of the “data protection” rubric based on the “right to control how information about you is used”.⁴⁰ The legislation around data protection, when described as “privacy” legislation, has a tendency obscure that a particular narrow sense of privacy is assumed: that of protecting personal information.

Even this characterization is somewhat inaccurate, as it is not “information” but data collections or records that are generally protected by the legislation, even when the term “personal information” is used. Unlike rights management schemes that operate in the private sector, such as Digital Rights Management, there is no technology to recapture lost information, or prevent it from being misused or decrypted. This is where the “custodial” metaphor breaks down. And similarly, the custodian is obligated to continue protecting data records that hold the information even after the information has been disclosed (perhaps inappropriately) and become public knowledge. It is the obligation to follow certain prescriptions in the management of data – not information per se – that has become paramount.

Another way to critique this same paradigm notes that the health information legislation is primarily providing additional exceptions to the consent requirements: that is, it is designed to protect the custodian that cannot feasibly obtain consent for the use of data. Instead, they must

behave in ways the legislation interprets as reasonable. It is incidental that this should also protect the individual's information, by encouraging reasonable behavior and safeguards around the data.

In health care, the data handling is often outsourced. The largest EMRs being constructed are handled by private vendors, and much of the information and data services will be provided in the private sector. The custodians of information are not the ones providing the technical solutions to protect or manage the data. The caregivers – the custodians – are not the technology experts. This is one of the problems that arise with outsourcing in general; the actual securing of data and enforcing appropriate access to the information is not directly in the hands of those with statutory obligations, but in the hands of IT system staff or personnel. When the information service is outsourced, this means many obligations are outsourced with it.

In health care, the issue of whether contractual obligations are adequate substitutes for statutory obligations arises, as it did in the public/private legislation comparison. One of the differences in this context, however, is that much of the legislation requires specific privacy protection in the contract language, which makes it far less likely that the contract will fail to include privacy protection elements.⁴¹ Furthermore, some statutes create custodial obligations for such contractees directly in the statute,⁴² creating statutory as well as contractual obligations on the part of the outside service provider. Of course, this still does not resolve the concerns regarding economic motivation of private entities, or the difficulty of ensuring compliance with their obligations.

Using data protection as a surrogate for privacy may give a superficial appearance of protecting other personal values such as confidentiality or trust that are not necessarily addressed. Neither patients nor physicians necessarily believe that confidentiality or trust are properly construed in a data protection scheme.⁴³ The people required to “trust” the system with their personal information and the professional who use it to ensure confidences are not the ones who control the outsourced system or know how it works. Therefore, the legislation protects the provider – the health care professional – from breaches of personal information as long as they have acted according to their statutory obligations. The responsibility for actually securing or protecting the data is out of their hands – and in the hands of private industry, which is responsive to the imperatives of the marketplace.

The security and privacy technology deployed creates a parallel appearance of a substantial effort to protect privacy, which in the case of Health Canada Infoway's privacy architecture, presents an infrastructure surrounding privacy that is relatively intricate. But there is always a danger that the appearance of increased complexity is a substitute for improved privacy protection. And it should not be allowed to obscure the fact that explicit or implicit interpretation of policy is made by the choice of technologies implemented and how they are implemented – which is often where the expertise of private industry is engaged.

An example of such interpretation is the technological treatment of consent. The use of consent directives recorded in the system to identify implicit, express, or lack of consent for particular uses of personal information and check them against the appropriate legislated requirements is one type of technology that is advocated, under terms such as e-Consent.⁴⁴ But if individuals do not really understand the risks inherent in the system or its operation, it is difficult to ascribe meaningful, informed consent to their choices. Furthermore, there is some indication that individuals simply will not want to provide a long list of nuanced consent choices: but that does not mean they won't be upset if their privacy is compromised. If such concerns have merit, such an e-consent system may be less effective than it appears in terms of the individual's desire for privacy.

Another way technology casts its influence on policy implementation is in terms of the conventional paradigms for protection. The notion of a "perimeter" of protection (a concept that grew out of private business concerns) fits conventional security, and aligns well with the "circle of care" notion, but may create a predisposition to think of privacy in those particular terms. For example, it was common among privacy policy administrators to think of internal breach – i.e. inappropriate access by those in the institution – as a privacy issue, whereas an external breach – such as someone "hacking into" the system – as a security issue. And this is reinforced by technologies distinguish authentication (who are you?) from authorization (what are you allowed to do?).

A tendency among the service providers to favor established technology solutions is also a concern. In many respects a conservative approach to technology deployment is beneficial: one wants to use proven, known solutions rather than risk unproven "bleeding edge" solutions. Furthermore, vendors are more comfortable selling solutions and systems they have experience

and expertise to build and support. However, this means there is a systemic reluctance to consider truly innovative approaches.⁴⁵ In addition, there can be economic disincentives against innovation in an outsourcing context. For example, vendors who are providing data services have an economic motive to prefer centralized data housing over a system that distributes data across independent systems, regardless of security or privacy implications. The more data they cluster in their own service points, the larger their service fees become. It is noted that the Infoway Architectural Blueprint has centralized registries as a key feature of its design.

Such technology choices that have substantial impact on privacy and security exposure are left late into the project development, so it is the project staff or technology experts that therefore make the technology deployment decisions that have substantial impact on privacy outcomes. It does make sense that policy is not prescriptive when it comes to technology choices: but at the same time, if technology is mediating the meaning or impact of the policies there needs to be some means of considering that function.

One of the types of choices that is left to policy administrators is whether a privacy requirement is implemented as technology, training, institutional protocols or enforcement procedures. This kind of choice makes is critical in terms of how risks are balanced. For example, access control technology and passwords can enforce usage restrictions on health care workers, where training and protocols would rely on individuals to respect the procedures put in place. This is largely a matter of how trust is distributed among the “circle of care”, and allocates risk of exposure of personal information accordingly. It also indicates that the private service provider should not be making these decisions based on technology preferences simply because the cultural issues surrounding privacy haven’t been addressed as a specific policy choice.

5.3 Advantages of health care privacy regime

Along with the concerns that a look at the health sector raises, there is many areas in which the privacy regime in health care provides examples of effective application of privacy principles.

There is a high degree of oversight and review activity in health care: specific privacy officers or their equivalent exist in all major institutions with a clear identification of their roles, responsibilities and the legislative requirements to which they are responsible (although small private clinics are not as active), and Privacy Impact Assessments are understood and used in all major information technology projects in health care that we encountered.

There was a correspondingly high degree of interest and active involvement in issues regarding consent, privacy and access, the accuracy of data and its impact on the existing system by nearly all stakeholders. Undoubtedly, not only does the nature of the legislation and the visibility of Infoway's efforts have a positive impact here, but also does the fact that privacy, confidentiality and personal information have a critical role in the structure of health care delivery. There are a variety of different entities involved in addressing these issues, from practitioners, administrators and technology experts to ethics review boards and advocacy groups.

The health care system exhibits a complexity of functions and scale that would be seen in very few other sectors. It is accordingly well resourced in a number of senses. Certainly for health boards and institutions, there is a large administrative capacity available to undertake at least some of the privacy oversight functions that are necessary. Even if data services are outsourced, there is little likelihood the private vendor would operate without some degree of scrutiny, since data would be moving back and forth as personal health information is accessed and updated. This is not to claim that health care is sufficiently resourced for new data protection governance and oversight responsibilities: but it has infrastructure that is visible and available to address these issues.

There is also a relatively high degree of understanding of privacy issues in health care. For example, nearly all stakeholders can describe some conceptual difference between security and privacy, a distinction that can be problematic for the layperson. These often represented different viewpoints or had import or subtle differences, but there were no characterization of privacy as simply one aspect of data security.

This can be contrasted with efforts such as the Transport Canada led project involving data collection for the No Fly List.⁴⁶ Driven by political need of sharing information more broadly, the lack of a conceptual PIA early in the project failed to bring out the fundamental privacy issues. More significantly, this initiative reveals a theoretical underpinning that assumed improved security (in the sense of national security) entailed sacrifice of privacy on the part of individuals. With such a conceptual base, an examination of possible technical solutions around data collection, retention and access that would preserve privacy was unlikely. There was little consideration given how state security and the protection of individual privacy might be met as

dual goals.

In the health care regime, no gaps were found in the delegation of responsibilities for privacy oversight or protection. One might take issue with how policies or legislation was interpreted or implemented, or if the responsibility is effectively left in the hands of private enterprise, but there were no situations in which obligations were not being addressed because the locus of responsibility was unclear.

There was recognition of overlap between personal and professional obligations and privacy protection, and that these obligations are not always complementary. The issue of conflict between professional values and requirements of the EMRs arose: for example, it was clear if access control technology compromised patient care, the professional imperative of the physician demanded that the technology controls be circumvented. The solution to these conflicts was generally not satisfactory to one party or another, but the conflict itself was recognized and debated.

There was also a high degree of interest in understanding the legislative requirements surrounding privacy. Perhaps this is a matter of health care's substantial exposure to litigation and the high degree of public interaction. These may not be factors in other application areas.

The example of Health Canada Infoway in the development of EMRs is instructive not only for the warnings about limiting policy perspective to "data protection", but also for positive aspects it exemplifies: it *is* possible to incorporate privacy and technology issues as a integral part of project development; architectural frameworks *can be* in place before deployment of technology and form the basis of further discussion; industry *can be* brought into the discussion of technology evaluation before contract stages; but the public sector has to expect to take the lead in this collaboration. In the next section, public and private sector influences on technology innovation is examined through a particular example.

6 Technology, Standards and Innovation

Privacy protection in data services is a relatively new application area for computing technology. Security measures, based on the idea of preventing unauthorized access to

proprietary data, have been around since the first password was used. More recently, there has been rapid development of new technologies that extend the “secure perimeter model”, not only addressing secure communication in a networked world, but also trying to protect identities and control partial disclosure of information as a means of privacy protection. Our previous work represents one effort to catalogue these technology developments.⁴⁷

Some of the relevant technologies are well established: data and communications encryption, public-key cryptography, digital certificates and secure remote access are now “off-the-shelf” components for networked applications. Authentication, authorization, activity logging, malware detection and data archiving are all well established technologies that a competent “outsourced” service provider should offer in their solution suites. At the other end of the spectrum are “immature” technologies that are being considered but have little track record of adoption in successful in working systems: trust management,⁴⁸ privacy-preserving data mining, and privacy rights management are examples of these. Occupying a middle ground are technologies that appear ripe for deployment, but have not yet established dominant conventional solutions in the marketplace. User identity management and consent management are in this category.

In the case of well established technologies, they should be well enough understood and evaluated that they could be adopted in outsourcing documents and contract language when appropriate. Known commercial implementations (like virtual private networks for remote access) could also be identified, and any oversight or audit necessary for compliance (such as logging, tracking or indexing methods).

But there appear to be no privacy technical standards to apply either to contract or oversight, in the context of PIAs or contract requirements. Nor is there consensus about the definition of what a privacy technical standard would include. If you approach privacy merely from a ‘data protection’ mindset, existing security standards⁴⁹ and solutions answer many of the concerns. However, privacy technology, when distinguished from security technology, suggests different technology concepts - such as unlinkability, de-identification, and data minimization. These concepts require and drive very different architecture designs and technical tools, and can produce different technical outcomes.

In their 2006 Audit report on Large Technology projects,⁵⁰ the Auditor General concluded

that there were difficulties with the management of technology projects in the government more broadly. This report found, with notable exceptions, that the business cases had been insufficiently articulated, most projects suffered from a shortage of qualified personnel as well as a wide variety of project management practices. It stands to reason that if the fundamental elements of an IT project are found lacking by the Auditor General, the more nuanced issues like privacy and privacy technology solutions are especially vulnerable.

The lack of privacy technical standards or guidelines makes it difficult for government agencies to assess tender bids or even construct relevant RFP requirements in the first place, at least on an objective technical basis. An alternative approach which also provides for discussion on a technical level is development of a reference architecture or technology, as evidenced in Infoway's privacy and security architecture. Such reference architecture provides valuable guidance for technical requirements, potential vulnerabilities as well as technical tools needed to provide specific services. A privacy reference architecture would also allow developers to match their proposed solution against an objective technical "roadmap" to ensure consistency, sharing of best practices and solutions

A third element common to technical development is testing or evaluation suites – software that will test the deliverables. These might not be feasible to develop pre-contract, as they require specific requirements to be well defined and detailed, but it does represent the most technically precise way of defining successful implementation. Similar but less specific evaluation schemes or criteria can be developed in more general terms to be included in contracting or outsourcing decisions.

Such efforts to classify, categorize, or evaluate privacy technology have potential benefits in sharing knowledge and solution not only among non-specialists in government departments and different projects, but also between clients, private sector vendors, and industry as a whole as a basis for discussing technology solutions using a common language. Even a basis for understanding what technology choices are available and how they relate to privacy objectives could be beneficial.

The cataloguing or organizing of choices has attendant risks, however: as technology is constantly changing, a canon of technologies, if not constructed carefully, may tend to exclude new innovations or marry solutions to a prescribed set, excluding new technologies as they

arrive. In addition, adoption of particular solutions may circumscribe policy choices.

In the following section, we examine a particular example of a technology that is currently under development and being considered for deployment: e-Consent. This technology is of particular interest because not only because it is currently expressed using different strategies in different places, but also because there is concerted effort to apply this concept in the health care context. Thus, we expect it to be illustrative of how very specific technology choices can interact with policy directions.

6.1 *The story of E-consent innovation*

There is little evidence of any work on e-consent prior to the early 2000s. Perhaps the earliest effort comes out of the Australian Department of Health and Aging beginning in the late 90s. This initiative was based on the premise of a distributed electronic medical record and health record, with some tracking of patient consent built into the infrastructure.⁵¹ In this initiative, patient consent was implicitly represented in e-consent objects.⁵² Such objects, when attached to stored medical data, would indicate who was permitted to access the data and what they could do with that data. Similar in concept to certificate mechanisms in digital rights management (that prevent you, for example, from playing downloaded MP3s on your computer without the appropriate digital certificate), such a design accommodates the complexities of medical data, including consent that might originate from a different source than the information, or might be implied by statute.⁵³ A copy of the e-Consent object is to be obtained and consulted when the data is accessed. For enforcement purposes, this relies on the software that accesses the data behaving in compliance with these e-Consent rules.⁵⁴

The e-Consent object is more flexible than the conventional approach of building consent management as an extension of role-based access control (RBAC). Under RBAC, user access to sensitive data is authorized on the basis of the user's role (such as administrator, physician, technician, and so on). It is relatively easy to record consent as permission given to access data entries on a role-by-role basis. Assuming the RBAC roles are recorded in a database system, it is a simple application of existing technology to add permission information to the database as well, providing the basis for an RBAC e-Consent solution. The e-Consent object, being inherently distributed and not restricted to role-based consent, was a much more innovative design.

A number of demonstrator systems were built under the auspices of the DoHA.⁵⁵ Preliminary research by DoHA identified that “clinical settings are highly diverse and an enormously wide range of challenges arise” which could not all be addressed by their research efforts; moreover, there were no off-the-shelf solutions that could provide e-Consent in health care or even formal frameworks for consent in privacy-related systems in general.⁵⁶ These demonstrator systems were tested in various Australian states, and this testing phase concluded with a series of reports and workshops to discuss the project results.⁵⁷ Interestingly, the DoHA reports have become difficult to obtain, reputedly due to changes in government policy.⁵⁸

In the design of these demonstrator systems,⁵⁹ four types of patient consent were identified: blanket consent; general consent with specific denials (an “opt-out” type of framework); general denials with specific consent (an “opt-in” type of framework); or a general denial. Looking at the function of e-Consent, there were also different possibilities: as a “legal record”, the person accessing would simply be notified of the legitimacy of their access as it was recorded. A second alternative was for the system to actively audit access and actively notify an authority (possibly the patient) in the case of inappropriate access. The most comprehensive choice was a “gatekeeper” function which would actually enforce the access privileges according to the e-Consent object.

The Australian reports generally conclude that the correct balance between privacy and the need for access was met with the general consent with specific denials (a partial “opt-out”) framework under a “gatekeeper” model.⁶⁰ A second critical finding is that a decentralized or distributed data system using e-Consent could be easily adapted to a centralized setting, but a centralized or aggregate design could not be made to work in a distributed setting after its construction.⁶¹

Work on e-Consent in healthcare continued at a slower pace after the conclusion of the DoHA-sponsored projects. Despite the inadequacies of the off-the-shelf components, efforts were to retrofit working systems by modification of conventional technology such as RBAC.⁶² The result is something the designers dubbed an “anti-RBAC” model. In the general e-Consent object, consent may be given in terms of institutions, individuals, facilities: it is not limited to roles. To accommodate such a model, RBAC mechanisms were circumvented by defining a general “care team” role (reminiscent of the “circle of care”) and superimposing a more general

model on top of that role. Modifying the underlying role-based mechanisms was not without its difficulties, and met with limited success. The final exemplar of the Australian efforts was a prototype of a more general e-Consent object (called an e-Tag) that can also accommodate roles based as well as “anti-RBAC” consent rules.⁶³ An Austrian effort to develop a distributed medical record system⁶⁴ pays some deference to the e-Consent initiatives in Australia; however, the emphasis of this work seems to be on the distributed model of data as opposed to the consent mechanisms. There has also been some exploration of an “agent” approach to enforcement, where some aspect of automated negotiation would play a role in the controlling data access.⁶⁵

Even more radical attempts⁶⁶ to incorporate e-Consent have appeared recently as an application of aspect-oriented programming, which is a relatively new programming paradigm that attempts to separate concerns or aspects of a system that are pervasive throughout the system code. This contrasts significantly with conventional decomposition or modularization approaches, in which specific functionality is isolated in specific system components (for example, the privacy and security services module of Health Infoway’s architectural blueprint).⁶⁷ Clearly legacy or off-the-shelf systems cannot benefit from such new programming techniques.

There are clear advantages in using more conventional approaches, as they will more likely be able to accommodate legacy data systems and older data collections with less modification for refit. Electronic health records in England adopt this approach,⁶⁸ relying on centralized data aggregation antithetical to a distributed approach. The Canadian model as expressed in the HCI initiative could be described as a series of provincial registries that adopt the same aggregate data model, but need to be interoperable. In contrast, in the Netherlands, personal health information is remaining in its original distributed setting in clinics and facilities, as an infrastructure develops bottom-up to incorporate a distributed e-Consent mechanism. The aggregate data systems also have the practical advantage of easily extending existing solutions, such as RBAC, to provide an easily managed, centralized control over the systems. But they give up flexibility of allowing access directives to be based on criteria other than roles of the caregiver.

Many factors push the Canadian system toward an RBAC interpretation of e-Consent. Vendor solutions will tend to off-the-shelf, proven implementations, rather than a more flexible, distributed concept of e-Consent. This is simply a consequence of being able to deliver what they are familiar with and therefore can guarantee will function correctly. The economic bias of

service providers towards aggregate data solutions (as discussed previously) will also discourage distributed solutions with more flexible e-Consent approaches. Health Infoway has also been given timelines to complete its mandate, which discourages the risk associated with innovative approaches. The result is that innovation is effectively discouraged.

The initial message from the Australian effort bears repeating: a flexible e-Consent mechanism (i.e, one NOT tied to access roles) cannot be implemented form off-the-shelf technology.

The conclusion is that the effect of turning to industry (and therefore of an outsourcing approach) is typically to obtain conventional and established solutions. Vendors will sell what they have, and will not create new approaches unless they are paid to do so. In the case of e-Consent, the outcome is likely to be what is known to work: an RBAC-based consent with large aggregated data repositories. These technology choices are then policy choices: in this case, they prescribe what can be done in terms of preventing access of delineating patient consent.

None of the guidelines, mechanisms, legislation, or PIAs suggest that the policy implications of specific technology choices are important or targeted in an outsourcing process. Yet it is clear such a discussion is not only feasible, but often takes place: the “legal”, “audit” and “gatekeeper” functionality of the e-Consent system is an example of the type of decision that should have policy input, above the level of policy administrators. Instead, there is a danger that the high-level policy decisions revolve only around those narrow aspects of privacy and data protections we see reflected in the legislative instruments.

It is clear, however, that such implications of technology choices on privacy outcomes will not be addressed by relying on private sector companies to introduce innovative privacy-directed solutions. An examination of outsourcing in the context of project development follows in the next section, which may provide some insight into how such policy concerns might be accommodated.

7 Process Model and commentary

There are four main documents used in this section to construct a model of the outsourcing process with respect to federal projects involving privacy policy. They are:

- *Privacy Impact Assessment Guidelines: A Framework to Manage Privacy Risks*⁶⁹ (The “PIA Guidelines”)
- *Guidance Document: Taking Privacy into Account Before Making Contracting Decisions*⁷⁰ (The “Guidance Document”)
- *The Privacy Act*²
- *Audit Report of the Privacy Commissioner of Canada: Assessing the Privacy Impacts of Programs, Plans, and Policies, October 2007*⁷ (The “Audit Report”)

7.1 Project inception to contract: an idealized model

The project development process in a Federal agency is involved and complex: development of a comprehensive model of project development would be well beyond the scope of this work. What is offered is a view of project development reflected on the privacy and outsourcing aspects that are reflected in the guidance documents that are generally available. Diagram 1 depicts the steps that should be undertaken during project/program development with respect to personal information, and is focused on the role of the PIA in that process. This is drawn principally from the PIA Guidelines.⁷¹ The second diagram depicts the elements that are part of the consideration of the possibility of outsourcing, according to the Guidance Document.⁷²

Development of Federal Programs Concerning Personal Information₍₁₎

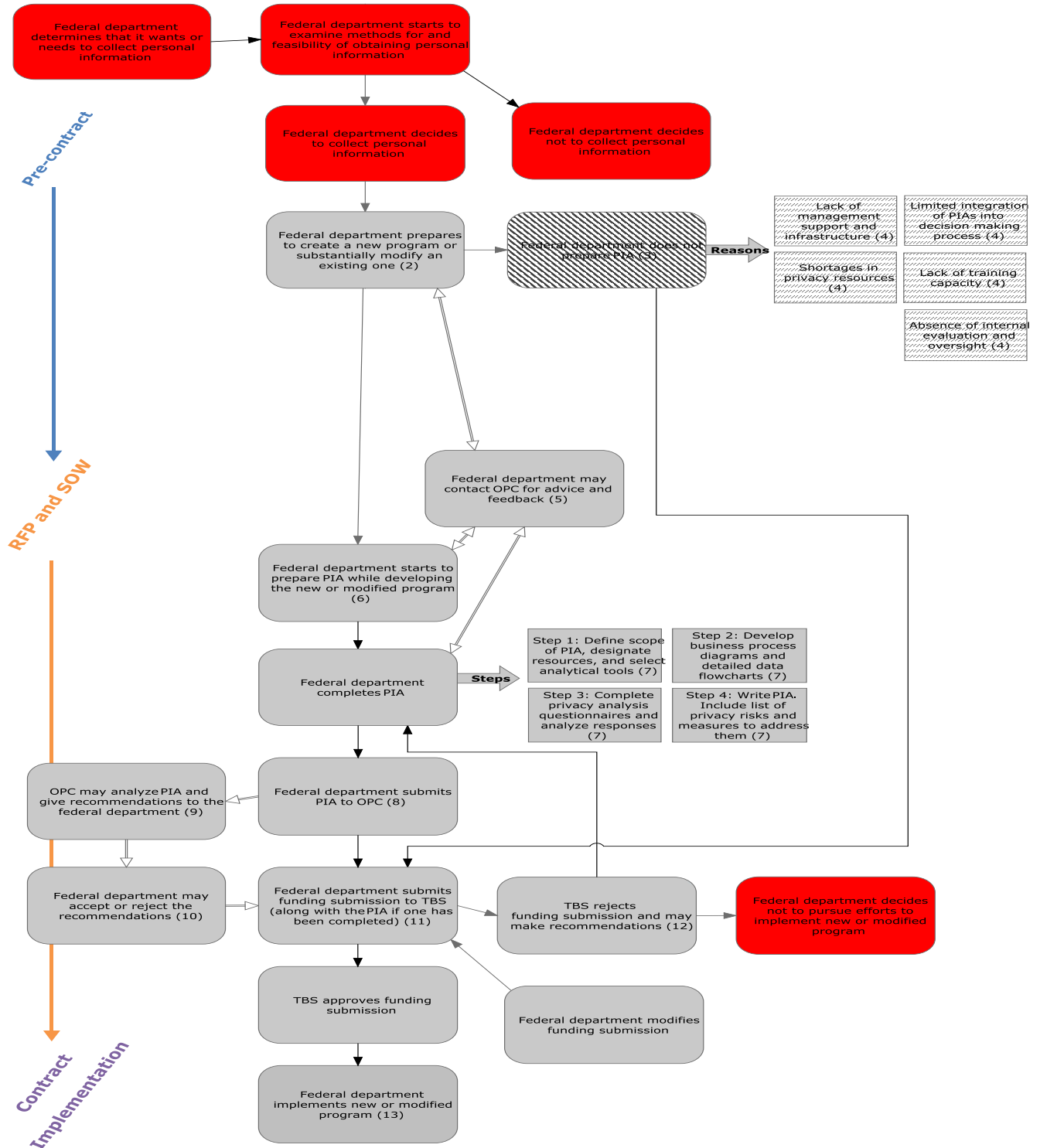


Diagram 1

Outsourcing involving Personal Information

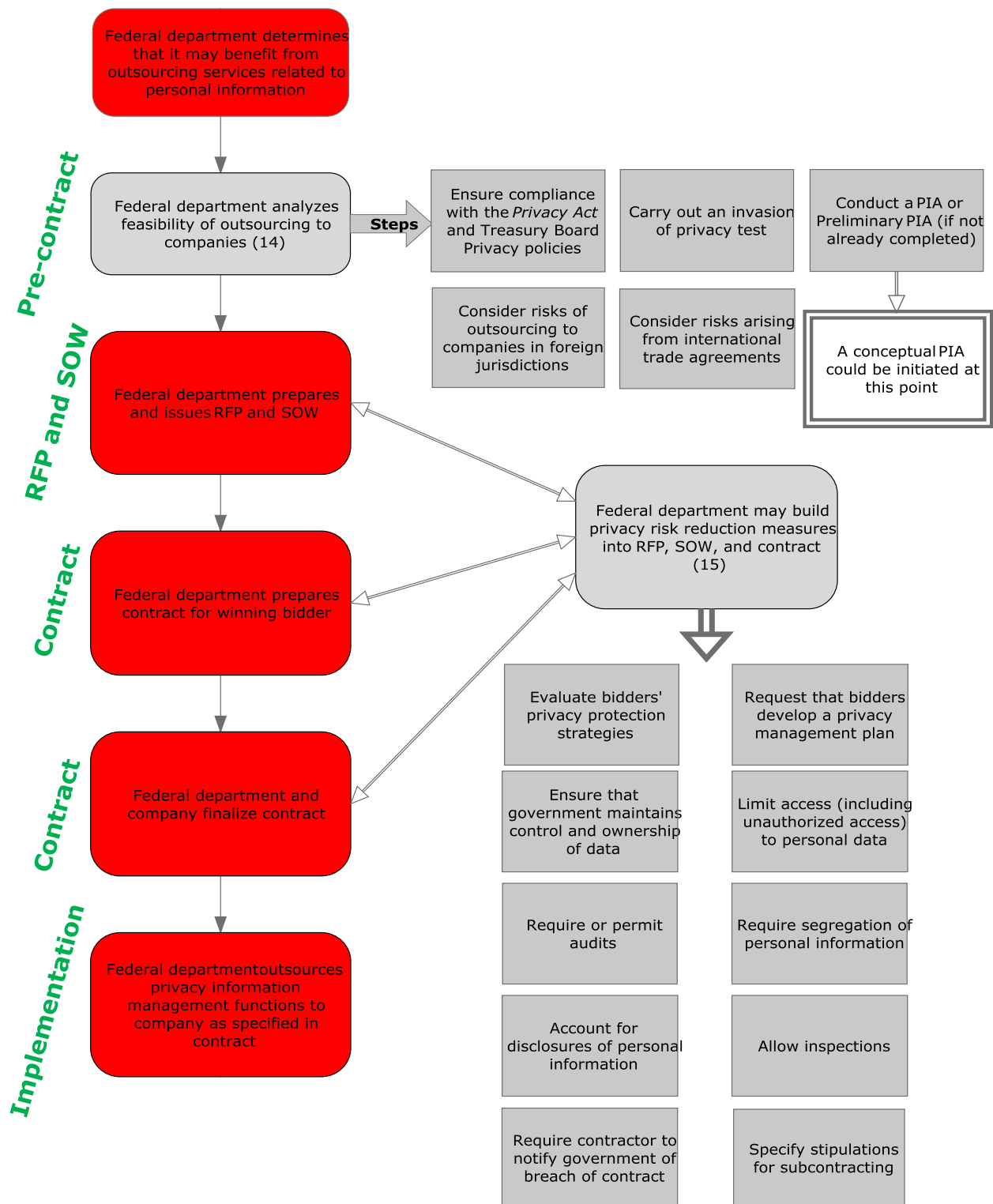
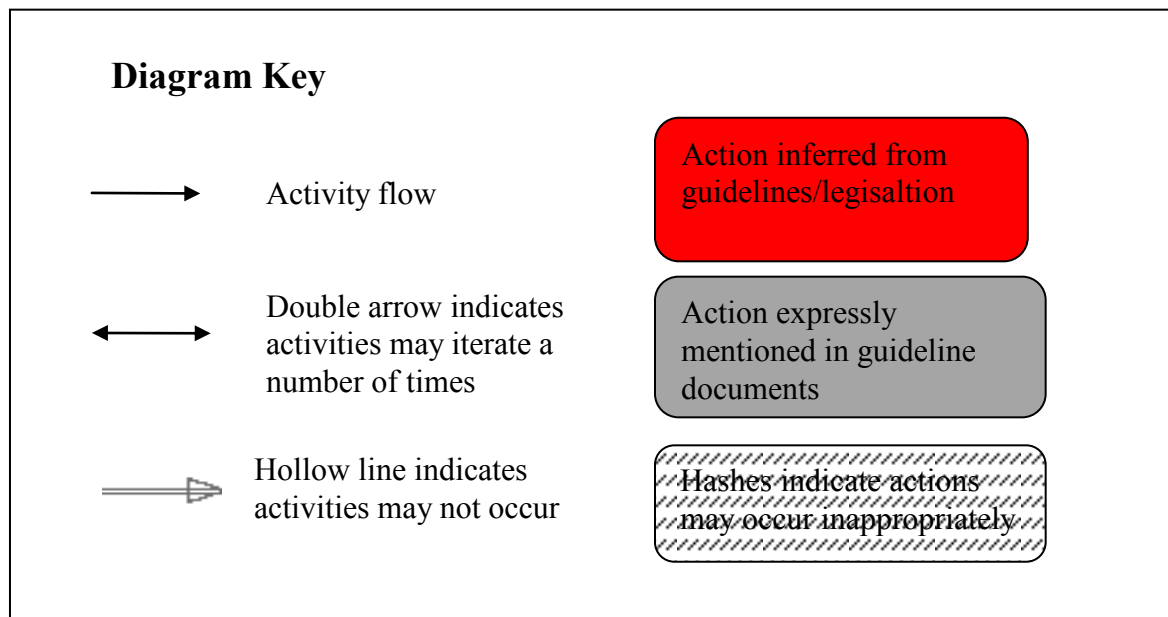


Diagram 2



The actions shown in these diagrams are generally inferred from the federal privacy documents, which prescribe guidelines for action as opposed to providing comprehensive lists of activities that must be carried out. For example, the Guidance Document suggests various privacy risk reduction measures be considered in RFPs, SOWs, and contracts. However, the actual process for preparation of RFPs, SOWs, and contract preparation are not specified in these documents – the constraints and guidance for these activities involve many pieces of legislation and documents,⁷³ some of which will be specific to particular departments. This means the model, by necessity, does not yield a complete overview of the outsourcing/contracting process. A comprehensive study of the government contracting process is not represented here.

Some activities are clearly indicated in the guidelines, while others are inferred in the diagrams as necessary to provide a framework for placing where other activities might occur. Presumably, the comprehensive investigation suggested above would replace some of these “inferred” steps with more concrete and specific examples that would help highlight opportunities to incorporate the privacy and outsourcing problems in a real context.

Some steps involve a co-operation between entities which can involve an ongoing (double-arrow) exchange; some do not. For example, TBS approval for a funding submission is a one-way decision; implementation of the program does not result in another funding submission.

However, if a federal department contacts the OPC for advice, the OPC can contact the federal department to provide suggestions in a collaborative, back-and-forth effort.

7.2 Intersection of program development and outsourcing processes

These diagrammed views of outsourcing evaluation and program development process clearly overlap in time. Although diagram 1 indicates a point at which the outsourcing evaluation might be incorporated, it is clear that the tasks involved have to move through the phases of pre-contract, SOW and RFP process in concert. There is little guidance regarding how these activities might be integrated with privacy requirements.

In other words, there is no typical or required PIA implementation path. “If the initiative is at the early concept or design stage and detailed information is unknown, then departments and agencies should consider conducting a Preliminary Privacy Impact Assessment (Preliminary PIA).”⁷⁴ The guidance documents recommend that a Preliminary PIA be considered at the initiation of the project if the privacy implications are not already clear: this will determine whether a full PIA is necessary. There is no specific requirement that a full PIA be planned at the beginning of the project. While some projects start PIAs as soon as possible, others proceed well down a development path and must then attempt to retrofit privacy assessment into the program after privacy policy and technology decisions are made.

Pre-contract Stage

The pre-contract stage includes analysis of the feasibility of outsourcing personal data management functions to private companies. This is an early stage of the outsourcing process and would ideally intersect program development at a similar stage. The intersection may depend on how a federal department conceives a given privacy requirement; therefore the stages in the program development chart are shown as a “range”. This stage ends before a federal department decides to go ahead with implementing a new or substantially modified privacy-related program involving outsourcing. At that point, the federal department should have enough data to decide whether it wants to outsource federal information.

RFP and SOW Stage

The pre-contract stage is followed by the RFP and SOW stage. Again, the RFP/SOW activities are not explicitly tied to any particular element of the program development activity. As with the pre-contract stage, the RFP and SOW phase is shown within a possible range along

the program development process.

Contract Stage

When the RFP and SOW stage ends and the contract award stage will begin is also unspecified in the program development diagram. The contract stage would presumably have to follow the RFP and SOW stages. If the RFP and SOW are completed early, the contractor could be involved in any point in the development flowchart after the pre-contract stage. It is doubtful, however that the contract would be executed prior to approval of the TBS funding submission. Otherwise, there could be would be no funding for the new or substantially modified program (and thus no funding for the contractor). The contract phase therefore also appears in the last stage of the program development flowchart – program implementation.

Implementation

The implementation phase of the outsourcing process occurs after the contract is finalized. This implementation phase intersects with the final step in the program development flowchart.

7.3 Privacy in program development

A new federal program or modification of a program that involves collecting personal information (diagram block 1) should engage the program development process outlined in Diagram 1, starting at block (2). The *Privacy Impact Assessment Policy* states that “Departments and agencies must conduct Privacy Impact Assessments for proposals for all new programs and services that raise privacy issues. For programs and services implemented prior to this policy, institutions must undertake assessments if they are substantially re-designing them or their delivery channels or transforming them for electronic service delivery in a manner that affects the cancellation, use, or disclosure of personal information.”⁷⁵

The current PIA policy and guidelines date from 2001 and direct government departments to “consider” conducting a PIA in any new or substantially modified program, and to integrate this activity in the early stages of the initiative. If there is no recognition that personal information is involved, a PIA may not be done. Further, there is no recognition that PIAs may have different levels of specificity – language in the privacy community generally talks about different types of PIAs (conceptual, strategic, process, technical) which is not addressed by the guidelines; nor at what specific stages it starts prior to program launch, or what specific consultations are required.

As noted at blocks (3) and (4) in the diagram, the Audit Report notes that in many instances, federal departments do not prepare PIAs when they should. The Audit Report also says that PIAs are sometimes not started until after project conception or design. “While in rare cases, such delays were based on the absence of information required to conduct the PIA, more often the delays in privacy impact assessment were unrelated to challenges in gathering data.”⁷⁶ Possible explanations of the lack of engagement are shown at block (4)⁷⁷

The “Office of the Privacy Commissioner should be involved at the earliest reasonable stages of the development of Preliminary Privacy Impact Assessments or Privacy Impact Assessments.”⁷⁸ This intention is reflected in block (5) of the diagram. In reality, PIAs are sometimes not started until after project conception or design. “While in rare cases, such delays were based on the absence of information required to conduct the PIA, more often the delays in privacy impact assessment were unrelated to challenges in gathering data.”⁷⁹

The *Privacy Impact Assessment Policy* is quite explicit in defining when a Privacy Impact Assessment is required, (as would be expected to engage at block (6)). A PIA is required when a proposal to re-design a program or service involves:⁸⁰

- a new or increased collection, use or disclosure of personal information, with or without the consent of individuals;
- a broadening of target populations;
- a shift from direct to indirect collection of personal information;
- an expansion of personal information collection for purposes of program integration, program administration or program eligibility;
- new data matching or increased sharing of personal information between programs or across institutions, jurisdictions or sectors;
- development of or a new or extended use of common personal identifiers;
- significant changes to the business processes or systems that affect the physical or logical separation of personal information or the security mechanisms used to manage and control access to personal information; or
- the contracting out or devolution of a program or service to another level of government or the private sector.

The suggestion of a “preliminary PIA”, as show in diagram 2, might fit well in the process around block (6) of diagram 1. While the TBS recommends that PIA be initiated early on, it is not required. The OPCC has commented that if a conceptual or strategic PIA is conducted more informed policy decisions could be made and appropriate technology designs implemented. Through initial consultations, the OPCC office has been able to modify projects before problems arose.

One issue that arises is the content of a conceptual PIA. Since this term is in common use, but not defined, it is unclear whether a conceptual PIA is a more abstract concept than a full PIA, and whether it contains technical elements or not – usage seems to vary. It is not clear that a final PIA submission is any less “conceptual” and more concrete than a preliminary one.

The four core steps to complete a PIA required by the guidelines are shown in block (7). However, the Audit Report notes that “none of the departmental summaries we reviewed on-line contained more than a project description and a simple conclusion or disclaimer.” This suggests that the detailed steps to write a PIA outlined in the PIA guidelines are not generally being followed, or the lack of any impetus to make the results of assessments public in any substantive manner.⁸¹

Block (8) illustrates the requirement to “provide a copy of the final Privacy Impact Assessment to the Privacy Commissioner.”⁸²

The Privacy Commissioner of Canada may review PIAs and Preliminary PIAs to “provide advice and guidance to institutions and identify solutions to potential privacy risks.”⁸³ The Audit Report admits that in certain cases, this advice may not be given until well after the new or modified program has been implemented due to limited resources in the OPC.⁸⁴

Although all PIAs must be submitted to the OPCC, and the office attempts to review as many programs as possible, particularly those deemed sensitive, reports indicate that not all PIAs are thoroughly assessed. Since the comments and recommendations given by the OPCC are not binding, the process does not compel expedient review. Often called upon to answer the most basic of privacy questions, the resources of the OPCC are stretched beyond their mandate. In some respects the OPCC is being used as a PIA quality control mechanism as multiple PIA versions are submitted for comment and review. In this sense, the consulting services of the OPCC are being used to supplement internal knowledge indicating a lack of capacity within the department. Block (10) reflects that none of the major privacy documents say that recommendations from the Office of the Privacy Commissioner are binding, only that they must consult.

A PIA may be submitted to the TBS with project funding request, or the TBS could take the step of requesting one after submission. (Blocks 11-12)⁸⁵ Upon analyzing a funding submission, the TBS may request that a PIA be completed.⁸⁶

If new funding is required the department must indicate to TBS that a PIA has done. Despite this requirement, there is no clear understanding how the submitted PIAs are assessed by TBS. The policy is directed to department deputy heads to allow them to independently assess what privacy risks are acceptable within the initiative. This leeway allows departments to independently evaluate the risk and accept the risk in trade of for other factors or motivations including efficiency, cost or policy.

If a PIA has not been completed after the new or modified program begins, the federal department could decide to fulfill its obligations by preparing a PIA after the fact (Block 13). “In several institutions we noted instances where Privacy Impact Assessments had not been conducted until well after a project’s full implementation.”⁸⁷

7.4 Outsourcing the privacy impact assessment

There has been increasingly frequent use of external PIA consulting emerging from the TBS PIA requirements. Departments and agencies, particularly smaller organizations, feel they do not have the internal capacity or expertise to conduct the required PIAs themselves. The hiring of a consultant may be viewed as more efficient and quicker than relying on stretched internal resources.

However, a rather odd situation arises when the PIA is itself outsourced. A properly conducted PIA should create awareness of the privacy requirements and obligations within a department and enhance understanding of the privacy issues within the project team. When the PIA activities are outsourced to private consultants, the department often fails to develop internal expertise and awareness of project privacy issues.

PIAs can be out-sourced, conducted and submitted to OPCC or TBS with little or no review by the originating department. While the use of external consultants is a practice likely to continue, it would be helpful if there could be guidance given to departments engaging these consultant on how to reintegrate the knowledge and make technology decisions.

The overall impression of the outsourcing model is one of confusion: while the guidance documents themselves are relatively clear, without mandatory assessment and review with real consequences for the process, timing and content of assessments will be inconsistent. Furthermore, the level at which technology implications have to be addressed remains vague. The case studies that follow examine how the process has played out for specific projects.

8 Contractual and Outsourcing Experiences

Three case studies were undertaken to examine the dynamics of the outsourcing process. Interviews were undertaken with government and industry staff to obtain insight into how the outsourcing process engaged privacy concerns. The observations and comments in this section are drawn from those interviews.

- The Police Reporting Occurring System (PROS)⁸⁸ is the RCMP's new police records management system. Data sharing outside the agency is handled through the related National Integrated Interagency Information System (N-III) initiative.
- The Canadian "Do Not Call List" is a project under the auspices of the CRTC with major technical work outsourced to Bell Canada.⁸⁹
- The Receiver General Buy Button (RBBB)⁹⁰ is an electronic payment service used by federal departments and agencies for the electronic acceptance of payments and secure storage of related payment information

8.1 *The story of PROS*

The Police Reporting Occurring System or PROS is the next generation police records management system, replacing the Police Information Retrieval System (PIRS). Developed internally by the RCMP in the 1980's, PIRS isolated each police contact incident in vast information silos producing a large repository of duplicate information data that was unlinked. Each police contact required officials to re-enter data. In the initial system, data could be coded to limit or tailor the information that was presented electronically, thus recognizing that not all data was appropriate for all audiences.

In contrast, PROS was designed to automate linking and provide a single accessible file for individuals who have come into contact with police either as a suspect, victim, witness or convict. PROS allows for the creation, storage, update, maintenance, retrieval, sequestering, purging and disposal of information encompassing the entire law enforcement process. Authorized users have the ability to record and manage details of court proceedings from the time the original charges are laid through the disposition of charges. PROS changes the way records are managed, moving from a traditional paper based record to one within an electronic virtual records room.

Furthermore, PROS provides a common internet-based platform for sharing information

among federal, provincial, territorial and city law enforcement partners, including a range of public safety partners including court clerks. The RCMP allows only accredited law enforcement agencies to access PROS, as it was designed to permit police-to-police agency information sharing. The list of accredited law enforcement agencies may be extended based on future review.

8.1.1 PROS out-sourcing decisions and design

The development of a next-generation police records management system was too complex for RCMP internal development capacity. A commercial off-the-shelf records management solution was sought. Extensive RFP business requirements were based on experience with PIRS: the initial RFP listed 310 requirements of which three were withdrawn before the call process ended.

Upon review of the proposals the RCMP discovered that some of the identified business requirements were not available in off-the-shelf solutions presented by bidders. The products developed for a broad market base simply did not include the degree of flexibility and range of specifications the RCMP wanted. “The market provided us with the products from which we had to choose”, stated Superintendent Chuck Walker. In the end, requirements were relaxed to provide for one time data entry and a remote ‘all or nothing’ access system. Some business requirements did have to be met on delivery; the vendor continues to work toward these outstanding requirements.

The RCMP asserts that the power of the system is that it links information so completely and shares it broadly. The data entity (or collection of attributes) are entered once at a master level, and the resulting outputs are the information trees that connect relevant data together. The previous system, PIRS, was indexed to information stored in silos, thus allowing tailored restricted views of the information. The drawback was that PIRS required multiple searches to gather information on a single given entity, requiring additional labour in retrieval and validating the relevance of information.

Once law enforcement personnel are given access to PROS, they can see almost all data it contains. A limited mechanism can lock out highly sensitive files in their entirety; and data deletion is limited to personnel whose job function requires that function.

The PROS security module contains a limited version of Role Based Access Control. Actions (e.g., delete, add, view) can be limited according to the user role, but the type of information available for viewing (e.g., only firearms, only suspects, only witnesses) cannot be restricted.

Specific consideration was given to the security functionality of the system. Using a Virtual Private Network, a two factor authentication was deployed. All hard drives are encrypted.

Designed and implemented by Sierra Systems starting in September 2003, the initial \$12.5 million dollar contract⁹¹ included architecture, IT systems implementation, configuration, training as well as project office support. Sierra assisted in implementing PROS in 650 detachments over an 18 month period. There were over 130 personnel engaged, most of whom were contracted out. Eventually Sierra transitioned management to the permanent departments of the RCMP.

8.1.2 Usage and oversight

The RCMP allows police partner agencies to use the PROS system on a cost recovery basis, a benefit for police agencies that do not have an electronic records management system. The RCMP provides access to the PROS application and houses their data. These arrangements are articulated through MOUs making use subject to RCMP policies. The RCMP reserves the right to audit PROS use. Training is given for operation of PROS and policies around appropriate use.

Access to PROS system is managed by the RCMP Operations Systems Services Center currently under the leadership of Superintendent Chuck Walker. This team is responsible for deciding who gets access to PROS based on the job specifications. Talk about de-centralizing this decision making process raises concerns about possible loss of oversight and accountability. However, decisions to remove access (addition limitation on access) can be made remotely by other departments.

8.1.3 Outstanding access and privacy issues

Upon review of the PROS initiative, the OPCC advised the RCMP to build in additional role-based access control mechanisms that would allow for limited views. At this point, with the technology selection made and development already under way, the OPCC was advised that the

PROS technology could not be modified to limit access to specific predefined criteria (e.g., victim services, firearms). This outcome reflects that privacy implications and solutions not taken into consideration at the outset and built into an outsourcing contract will be expensive to correct.

With the deployment of the data rich PROS system, there is increasing interest by other non-police agencies such as victim's services and by-law enforcement officers to access PROS information. Policy clarification is needed whether these programs and services are properly law enforcement supports that should be given direct access to PROS; or that the level of data sharing PROS provides is not appropriate for these programs.

The issue of consent is most poignant with respect to victim information. Each of the 12 jurisdictions the RCMP works with has its own victims of crime legislation, and none address the privacy rights in the context of electronic records system. Since obtaining explicit consent of each individual victim is impractical, the all-or-nothing approach to data access under PROS creates problems for the sharing of data with victim's services organizations. The RCMP is currently addressing this issue in broad consultation with Provincial and Territorial representatives, RCMP Divisions as well as Federal, Provincial and Territorial Information and Privacy Commissioners. A PIA is being conducted.

8.1.4 National Integrated Interagency Information System initiative (N-III)

The National Integrated Interagency Information System initiative (N-III) is the next step in police data interoperability beyond by PROS. It extends data sharing, usage and interoperability while building in increased security and Governance Based Access Control (GBAC) features.

The N-III tool for information sharing among Canadian police services is the Police Information Portal (PIP). PIP is a query tool capable of accessing data in police Records Management Systems (RMS), including PROS, that are used by most Canadian police services. A single PIP query searches all participating agency PROS/RMS data and returns consolidated responses. PIP users can access more detailed information by using the drill down feature or by submitting a request for a report.

PIP is equipped with security levels which control the accessing of information. Participating police services configure security levels when initially arranging the PIP access. Users select the data that gets distributed through the PIP publishing option as they enter

occurrence data in their PROS/RMS system. This choice will be governed by the policy of the users' participating police service.

The Integrated Query Tool (IQT) ⁹² is the N-III information sharing tool for federal public safety agencies. This currently includes the RCMP and the Canada Firearms Centre (CAFC).

Participating agencies have access to RCMP occurrence data using the IQT. Within IQT, Governance Based Access Control (GBAC) tracks the legal restrictions for information sharing among federal agencies. GBAC controls the type of data that individual participating agencies may view, based on their legal authority. Access to data is filtered and formatted according to the mandate of the organization. Public Safety Canada is undertaking a PIA to consider the use of IQT by several public safety agencies based on their authority to collect information.

8.1.5 PIAs, the TBS, and the Privacy Act

Neither PROS nor PIP conducted a preliminary PIA. It was understood from the beginning that a full PIA would be required, which was deferred to a later time. Because there is no requirement or guidelines for either a conceptual or strategic PIA, the early privacy guidance those examinations might have provided was not available.

The RCMP personnel involved in the PROS initiative recognize the importance and value of a PIA. There is an acknowledgement that the PIA exercise can drive fundamental technology and architecture decisions. The PIA process, required to secure TBS funding, can be very helpful to compel decision makers to address the privacy issues up front and articulate privacy requirements at the same time and in the same light as other business requirements.

While the PIA Guidelines were helpful, it was noted that the documents were unwieldy and complex. There is also a concern that there are limited internal resources as well as external contract resources available to complete PIAs.

The observation was made that The Privacy Act is severely outdated and does not address the evolution of technology. RCMP personnel looked at other TBS policy documents and the PIPEDA for guidance.

There is a specific jurisdictional complexity with the PROS initiative as it involves federal, provincial and territorial users and therefore engages their privacy legislation. The interpretation of different privacy legislation by internal and external stakeholders can cause disharmony when trying to identify solutions or assessing requests for access to the system by "non consistent" use

groups. The conveyance of a unified position on “consistent use” and access to information systems by federal, provincial and territorial Information and Privacy Commissioners was cited as something that will aid the RCMP in its assessment process.

“The Operations Systems Services Centre proactively engages the OPPC and/or other Provincial and Territorial Information and Privacy Commissioners with respect to RCMP issues or initiatives that raise privacy concerns” states Susan Trautmanis, Legislative Conformity Manager, RCMP. “Having the opportunity for an early consultative process permits an up front assessment of risk from a collaborative perspective” she concludes.

8.2 The story of “Do Not Call”

The Canadian National Do Not Call List (DNCL) is a new project being spearheaded by the CRTC in partnership with its industry developer and administrator, Bell Canada. It has strong industry participation, particularly with the Canadian Marketing Association.

The Canadian National Do Not Call List has a long and detailed history. Producing legislative amendments and public and industry consultation over several years, the Canadian National DNCL program provides fertile ground for examining how consumer privacy protection and relevant technologies are implemented. The DNCL exemplifies negotiation among industry business needs and consumer protection requirements within a Federal legislative, regulatory and policy context.

8.2.1 Chronology of the DNCL

1. 1988 – CMA voluntary do not contact list established
2. March 2001 – CRTC began reviewing telemarketing rules
3. May 2004 – Issued Telecom Decision 2004-35 and subsequently stayed⁹³
4. November 25, 2005 – Bill C-37 – Royal Assent
5. Feb. 20, 2006 – public consultation was commenced
6. March 21, 2006 – Consortium of interested parties formed
7. June 30, 2006 – Bill C-37 – Amended legislation came into Force⁹⁴
8. July 7, 2006 – Request For Information initiated
9. Individual Vender consultation sessions

10. August 1, 2006 - CRTC Interconnection Steering Committee Do Not Call Operating Group (CISC DOWG) Reports
11. July 3, 2007 – Issued Telecom Decision 2007-48 which contains the National DNCL Rules and Unsolicited Telecommunications Rules framework (includes telemarketing rules).
12. July 30, 2007 – NDNCL RFP issued
13. September 10, 2007 – RFP closed
14. December 21, 2007 - Contract awarded to Bell Canada
15. December 2007 – development work begun
16. January 28, 2008 – Issued Telecom Decision 2008-6 dealing with the delegation of investigations of complaints about violations of the National DNCL and Unsolicited Telecommunications Rules
17. February 14, 2008 – CRTC issues RFP for a Complaints Investigator
18. September 30, 2008 – National DNCL Launch expected

8.2.2 Emergence of a Canadian model

The initial Do Not Contact list was developed and maintained by the Canadian Marketing Association, who also manage a Do Not Mail and Fax list. Adherence to guidelines is mandatory for all CMA members, but membership in the CMA is voluntary and only includes about 40% of marketing practitioners.⁹⁵

Its status as an industry initiative left the CMA with little substantive penalties for violators. The organization was in the difficult position of policing and sanctioning its own members. Eventually, the CMA encouraged the federal government to establish an official National Do Not Call list with investigation and enforcement powers that would encourage compliance by telemarketers.

The CRTC, the entity responsible for the oversight of telecommunication in Canada, began investigations into the establishment of a national do not call list in 2001 and was tasked with the development of the list through legislative amendments in June 2006.⁹⁶

In February 2006 a series of public consultations were held with formal presentations and submissions, mainly from industry organizations with a few consumer groups, notably PIAC (Public Interest Advocacy Centre), making submissions. In March 2006 a consortium of interested parties formed two CISC working groups. The first was tasked to address the possibility of the industry forming a consortium to administer the National DNCL. This group determined that the formation of a consortium was not possible due to the divergent interests of

the industry. The second group, the DOWG was tasked to look that the operations of the National DNCL and make recommendations to the CRTC. The CISC DOWG was mainly industry representatives (17) with only 2 consumer or citizen representatives. The consensus and non-consensus reports containing the recommendations from this working group were used to form the basis of the RFI and RFP.

In December 2007 a contract was awarded to Bell Canada to develop, implement, and operate the National DNCL as the CRTC's delegate. The third party investigation and complaints procedure delegate has yet to be decided. There is no governmental or CRTC funding for the development or operation of the National DNCL, although there was a nominal contract fee of \$1. All costs associated with the National DNCL will be borne by Bell Canada and in turn they will charge the telemarketing industry directly for subscription to the list. The CRTC will approve the fees Bell Canada will charge.

All persons or organizations who make telemarketing calls on their own behalf, and all persons or organizations who hire third parties to make calls on their behalf must subscribe and pay to download the National DNCL. There are several types of telemarketing calls that are exempt including:

- Calls made by or on behalf of registered charities.
- Calls made by or on behalf of political parties or political candidates.
- Calls made for the purposes of opinion polling or research .
- Calls made for the purposes of market research firms or surveys when the call does not involve the sale of a product or service.
- Calls made for the purpose of selling a subscription to a general circulation newspapers (but not magazines).
- Calls made to a business.
- Calls made to a consumer who has purchased a product or service, or had a written contract expire, within 18 months of receiving the call.

Violators who are corporations can be charged an AMP of up to \$15,000 per violation; a person can be charged and AMP of up to \$1,500. This money is payable to general revenues of the Federal Government.

Any Canadian telephone number can be registered, regardless if it is used with a land line,

a wireless phone, or a fax. There is no charge for consumers to register their phone numbers.

8.2.3 Implications of the DNCL

The technology services required include databases, an interactive website to collect data, on-line data downloads, on-line fee payments, transfer of certain payments to a third party Investigation Delegate, secure transfer of complaint data to the Investigation Delegate, secure transfer of data to the CRTC with regard to operations and statistics, an IVR system for consumers to register numbers and register complaints, and live operator services to register complaints.

Personal Information

For each of the services noted above the following personal data will, or may, be collected:

1. Registration of telephone number – only the telephone number
2. Registration of Complaints – telephone number is required as well as whether it is a business or residential number. Optional information includes name and postal address and/or another telephone number and/or email for contact purposes for contact purposes, language preference.
3. Telemarketer Information – personal information would be the name of the telemarketer's primary and secondary contacts. The remainder of the information is expected to be that of the Telemarketer's business (i.e. business name, address, telephone number, email, credit card information, language preference, Federal business number, etc.)

Out-sourcing

The ability to out-source the creation and operation of the Canadian National DNCL stems from the Legislation amended in 2006. The changes to the Telecommunications Act⁹⁷ included a section that allows the CRTC to delegate this work out to a third party and allows the third party to charge for exercising its delegated powers. The CRTC chose to exercise the option of out-sourcing for several reasons:

1. The CRTC does not have the internal capacity to develop and administer the list
2. They had the legislative power to delegate
3. There is an international precedence for out-sourcing National DNCL
4. The CRTC does not have the power to collect fees from telemarketers

Funding

Parliament's legislative intent was that the telemarketing industry fund the Canadian

National DNCL. This funding model is also used by the UK, Australia and to a different degree the US for their respective do not call lists. The CRTC receives its funding through fees imposed upon Broadcasters and Telecommunications Service Providers - it does not have the ability to collect funds from telemarketers directly. Unlike the US model, and ignoring industry recommendations, the Government of Canada chose not to provide start up funding for the National DNCL.

Without direct CRTC or GoC funding, the CRTC felt they were unable to establish and insist upon specific architectures or technical requirements. With no CRTC or GoC funding offered to initiate development and the cost recovery and with a revenue model whereby the fees established to fund the National DNCL would be approved by the CRTC, a situation was created where it is in the vendor's best interest to develop and administer the system as cost efficiently as possible to maximize quick returns on investment. A cost minimization incentive could be said to contribute to a lack of corporate interest in innovating privacy enhancing architectures and technologies.

International Vendors and Contractors

There has been consumer concern expressed about implications of the US Patriot Act on Canadian out-sourcing activities if the selected contractor was a US company, or it subcontracts work to a US Company, or if the data resides out of Canada. Due to the various trade constraints, including WTO and NAFTA, and the limited amount of personal information collected, the CRTC determined they could request that the data reside in Canada but they could not require it in the RFP. It was argued that a Canadian data residency requirement could be taken to the trade court as an unfair disadvantage.

Although the CRTC contractually requires that the National DNCL contractor comply with both the Privacy Act and PIPEDA, if the data were to be shared with any international data centre or service provider the ability to enforce the Canadian governmental legislation is compromised. In the case of the US, the Patriot Act can compel disclosure of the Canadian data.

In the successful Bell Canada submission they indicated that the data would remain in Canada, under Canadian legal jurisdiction. However, Bell Canada has indicated that a technical development partner is based out of the US. It is unclear at the point if the US sub-contractor will get access to the data for development, testing or QA purposes.

The Guidance Document has imposed very careful scrutiny over extra-territorial sharing of personal information, but does not explicitly prohibit it from occurring.⁹⁸ This is presumably now relates to the existing TBS practices of ‘risk mitigation’ assessment and strategy. They are in the process of developing additional guidelines.⁹⁹ TBS does have a security requirement checklist that is used to determine the level of security protection required for technology initiatives.¹⁰⁰

When consulted by the CRTC, the Public Works and Government Services Canada indicated that the TBS guidelines were to be followed, which implies a threshold test asking ‘if the data was released to a US company what is the harm that could be done?’.

The lack of clarity and strict interpretation of risk is confusing for departments and decision makers.

8.2.4 Implications of privacy and technology decisions

The Canadian Marketing Association has been involved with internal industry do not call initiatives since 1988. They implemented a non-legislated do not call list to which all CMA members were required to adhere. Their early championship of industry behaviour standards reflected a belief that consumer protection is a part of their mandate. Consequently, the CMA was heavily involved with the legislation leading to Bill C-37 and the National DNCL.

It was in the interests of the CMA to have the federal government take over the expense, administration and enforcement of a national do not call list. It was also in their interest to keep the design and process similar to their existing list, in order to avoid extra cost and confusion as well as additional privacy restrictions on business activities. The adoption of the CMA do not call model as the basis for legislation determined the fundamental direction for the privacy and technology decisions yet to come right from the outset.

The Do-Not-Call List Operations Working Group had several non-consensus items relevant to technology and privacy considerations.¹⁰¹ The issues debated under the database management area affected two fundamental technology and design decisions.

First, was the question of the technological alternatives and access architecture upon which to base the National DNCL list. There are two main methods. The first method ratified by the majority of the committee is the download method that is used in the United States, the U.K. as well as by the Canadian Marketing Association in Canada. In these implementations, users of the

DNCL download the list of numbers to their own systems and use it to scrub their own contact list. They then proceed to market to the remaining numbers. The known advantage of this method is that it is simple, proven, cheap to implement, and many Canadian telemarketers already have the systems and processes in place to assimilate this type of DNCL. In the second option, a query/response method championed by the non-consensus minority, a telemarketer would query the DNCL system with a number or a list of proposed call numbers. The DNCL system would then inspect the number(s) and inform the telemarketer if contact was permissible. Proponents of this method assert it is more efficient and cost effective system, as well as easier for small telemarketers to use.

In light of the strengths and weaknesses of both methods, the majority felt that bidders for the National DNCL Operator contract should investigate both proposals and determine the feasibility of either method, or a combination of both. It was believed that the feedback provided through this process would provide the CRTC (or a DNCL Consortium) with the necessary information to ultimately choose a candidate to become the National DNCL Operator.

The minority noted that permitting a commercial process to determine technology is, in effect, allowing a third party to determine public policy. The minority also believed that this type of fundamental design decision, which concerns the nature of a work solely intended to protect the public, should not be undertaken by the CRTC without carefully considering the opinion of well qualified, impartial, registered professional engineers.

Secondly, there was the consideration by the DOWG of the difference between a “Do Not Call List” and a “Do Call List”. It was asserted by the majority that Bill C-37 only allowed for the creation of a “Do Not Call List” and that no other registry design was contemplated by the legislative framing of the initiative. This was confirmed by the CRTC; we can observe how legislative framing directs the policy and technology outcomes from the outset.

There was a specific discussion about limiting telemarketers’ access to the National DNCL. “The majority was of the opinion that there was no security or privacy risk in the DNCL Operator implementing technology that would permit a telemarketer to download all or a portion of the DNCL....The minority remained concerned that telemarketers should not be able to download the DNCL from the operator because of the privacy risk of telemarketers having confidential telephone numbers.”¹⁰² This issue is subject is still under debate. If designers decide that phone

numbers are in and of themselves innocuous then the privacy considerations placed on them will be correspondingly small. However, if designers place those phone numbers in the broader context of other data banks, reverse look up technology, and re-identification attacks then individual data points could be increasingly sensitive and worthy of protection.

Pre Contract

In July 2006 the CRTC took the Do-Not-Call List Operations Working Group reports and ran a Request For Information from interested vendors and stakeholders. There were 11 responses that were used as a reference for the RFP. While some responses went into great technical details as to what code and tools would be utilized, others were more general in their comments.

While the RFI asked for general comment on privacy protection options, none of the industry respondents commented directly on how they would address privacy. All vendors proposed a version of the download model. Additionally, none of the respondents proposed any of the alternative privacy enhancing 'list scrubbing' do not call models or architectures. The lack of privacy preserving architectures and technologies at this stage limited the final technology requirements in the RFP.

The CRTC used a variety of external resources to frame the RFP. They engaged outside legal counsel and RFP consultants who specialized in government contracts to help develop the RFP and identify requirements in the RFP. The OPCC was asked to give informal guidance. PWGSC was also consulted in the process. The RFP was written and issued on MERX¹⁰³ by the CRTC.

Privacy requirements were not articulated for the vendors; instead the relevant documents from TBS, the Privacy Act and PIPEDA were referenced, and it was left to the respondents to translate the requirements into actions. The CRTC did have some informal consultations with the OPC and relied upon consultations provided by the PWGSC the external sources identified above to ensure the RFP included these references and included appropriate provisions regarding security and privacy from PWGSC's Standard Acquisitions Clauses and Conditions (SACC) manual.

Incorporating the above information as well as the DOWG reports and the information gleaned from the RFI responses, the bulk of the preliminary technical requirements were

synthesized at this point by Nancy Webster-Cole¹⁰⁴ building on her experience as a systems developer. Ms. Webster Cole also consulted with CRTC employees in the Telecom directorate and Informatics directorate who had systems expertise. The CRTC relied extensively on the expertise of external personnel to articulate the privacy requirements and obligations in the RFP. The CRTC clarified by the CRTC that the vendor must understand their privacy responsibilities on their own using their own access to professionals. It was also a requirement in the RFP that the vendor conduct a privacy impact assessment per TBS' policy.

The CRTC decided to separate the administration of the DNCL from the investigation and complaints procedure which has been recently undergone its own RFI process. It is unclear at this point how or if the administrator and the established DNCL technology will interface with the third party investigator. It remains to be determined how privacy enforcement compliance will be integrated if it isn't seen as part of the same process.

Contract

The CRTC evaluated the proposals based on relevant experience in developing, implementing, and operating systems similar to the system requirements of the National DNCL. Additionally, vendors were required to demonstrate that they could support the estimated costs for the first two years of operation, \$15 million. The actual estimated cost was not a factor for the CRTC in the decisions because the contract value was only for \$1, all risks for the costs lie with the vendor. As with the RFI, there were no innovative privacy solutions presented from any of the respondents; nor was there any expectation of such innovation required in the RFP – solutions were entirely left to the vendor. The CRTC professed no knowledge or capacity to mandate specific technology solutions. Proposals were evaluated based on experience with similar projects, and on December 21, 2007 the contract was awarded to Bell Canada.

Privacy Impact Assessment

The consulting group of the PWGSC recommended that a conceptual PIA be done. However, the CRTC did not feel that it was necessary as the technical architecture had yet to be

established.

As this initiative is well under way and most of the design and operational decision have already been made, there is little strategic input that a PIA can provide at this stage.

There is general misunderstanding of the role of conceptual PIAs to identify privacy policy and technical requirements. There was a lack of understanding of the types of PIAs and how continual and integrated PIAs can be used in the project planning and implementation process. The lack of a specific requirement for a conceptual PIAs leads to missed opportunities to make strategic decisions at a point where cost effective and efficient privacy solutions can be implemented.

Bell Canada will be conducting a systems and operational PIA pursuant to TBS guidelines. The RFP for the Complaints Investigator delegate requires the vendor to conduct a PIA. The CRTC will conduct a PIA for the enforcement process (which the CRTC is retaining) and any other new internal processes associated with the National DNCL and investigations. All three PIAs will be submitted to the OPCC by the CRTC.

The CRTC will ensure that the vendor complies (and continues to comply) with the privacy obligations through the PIA to be performed, performance audits, as well as third party security audits. There is an oversight committee formed with representatives from both Bell Canada as well as the CRTC who will review and sign off design documents and progress reports.

8.3 The story of the Receiver General Buy Button (RGBB)

Now part of the Secure Channel portfolio of services, the Receiver General Buy Button (RGBB) is an electronic payment service used by federal departments and agencies for the electronic acceptance of payments and secure storage of related payment information.

The personal information the RGBB deals with is credit card associated information including number, name and expiry date.

In 2006 Bell Canada responded to a RFP for the Government On Line electronic payment service with their Bell Electronic Payment System solution (BEPS). The original RFP was very vague as to privacy requirements, but its revision in 2007 added reference to privacy legislation and requirements.

The RGBB technology solution is based on a pre-existing commercial e-payment service

with some customization. There were no requests for additional security or privacy functionality beyond the off-the-shelf solution. This indicates that e-commerce transactions have reached a plateau as their use has become normalized. There is no industry push to ‘redevelop the wheel’ and there is no government incentive to create a new e-commerce paradigm.

Contract

The initial RGBB PIA indicated initial concern regarding a lack of privacy references. Specific wording was included in contracts to ensure the Vendor complies with all provisions of the Privacy Act.¹⁰⁵ The language added, like many of the standard clauses, indicates that the vendor must generally comply with all applicable privacy laws, but there is no specific reference to behaviour, technology or criteria. These clauses are vague and lack technical specificity.

The Statement of Work also indicates that the vendor must comply with current Payment Card Industry Data Security Standard (PCI DSS) – Level 1 (highest). The PCI DSS is a set of requirements for enhancing payment account data security. The standards, based on 12 principles, cover such aspects as security management, policies, procedures, network architecture, software design and other critical protective measures such as monitoring and testing networks. There is also an established system of third party audits that can be conducted to ensure compliance.¹⁰⁶

It is important to note that while PCI DSS represent the leading industry approach to data security, data confidentiality and data integrity they were not created to cultivate or protect consumer privacy. The use of the PCI DSS standards was an inadequate stand-in for privacy: data security does not always encompass privacy concerns.

8.4 Conclusions

Many common themes appearing throughout the report are reinforced from the case studies:

- A misunderstanding or differential understanding of the value of private data and privacy protection requirements can arise. For example, the data being collected by the National DNCL was ‘only a phone number’, it was deemed not to be overly sensitive data.

- The difference between security architecture and technology and privacy architecture and technology is not clearly articulated, so privacy may end up not being clearly addressed by technical solutions.
- Lacking a clear set of technical standards, the process may turn to security or industry standards, such as PCI DSS, which do not address privacy.
- Lack of Capacity
 - Smaller departments and agencies like the CRTC do not have the internal capacity to assess the privacy issues and take appropriate leadership – this is their primary motivation for outsourcing in the first place.
 - Smaller GOC department and agencies like the CRTC are dependent on external resources for legal and policy advice, RFP development and technology services. This dependence externalizes expertise and doesn't lead to internal capacity development.
 - Externalization of expertise may lead to an over reliance on industry vendors and advocates agitating for specific industry friendly solutions.
 - Lack of technical capacity and externalization of technical expertise leads to an inability to take technical leadership positions that would require, promote and advance the deployment of innovative privacy enhancing architectures, business solutions and technologies.
- Roles for consumer advocacy and external organizations.
 - There are few consumer organizations that are adequately resourced to effectively contribute to consultation processes
 - It is suggested that increased consumer involvement may counterbalance the tendency for choices to be industry driven and with little privacy consideration.
- Process weaknesses
 - The privacy technology options were limited by the historical precedent, legislation and heavy influence of industry
 - Conceptual PIAs were not used to provide early guidance
 - The technology choice process was idiosyncratic – there was no established process for technology choice discovery or decision
- Industry responses
 - The dearth of privacy preserving designs and technologies represented by industry solutions tends to limit their inclusion in RFPs and contracts, effectively limiting their presence in the final products as well.
 - There is a general failure from industry to offer innovative privacy enhancing solutions, although the government client tends to rely on the technology advice coming from the vendor.

Perhaps the common thread among most of these issues is the conflict between the need to outsource due to *lack of capacity* and the need to improve privacy oversight and assessment which dictates *increased capacity* and expertise. The current process structure does little to resolve this tension; it merely relies on those involved to adjust practices appropriately.

The case studies also produced a number of suggestions to address these concerns:

- Training in general to enhance expertise
 - for departments on the use of PIAs, conceptual PIAs and how to engage consultants
 - for RFP consultants -- departments without the internal capacity to articulate an enhanced privacy protection framework use consultants
- requirements specifically attuned to “conceptual” PIAs
- improved checklists and tools to assist with
 - the PIA process
 - assessment of privacy requirements, business processes, architectures and technologies when contracting
 - for TBS requirements
 - for Privacy Act requirements

Of course, the case studies also revealed the need to improve policy requirements and enforcement of the existing requirements in process, contract and PIA conduct and PIA review – but we would expect the participants to articulate the process weaknesses in terms of lack of resources, not in terms of lack of enforcement.

There are also broader concerns that are too diffuse to appear at the project implementation stages but are raised earlier in this document: the impact of outsourcing on public values, the structure of legislative instruments, reliance on a “data protection” as the only privacy perspective and the tendency of process to obscure the impact of implementation choices on privacy outcomes. These are the themes that drive the suggestions in section 3 of this report.

Notes

- ¹ The previous report, titled “Technology Choices and Privacy Policy in Health Care”, was submitted the Office of the Privacy Commissioner of Canada, and is available online: <http://cpig.cs.mun.ca/TechnologyChoices.pdf>.
- ² *Privacy Act*, R.S.C 1985, c. P-21, available from http://www.privcom.gc.ca/legislation/02_07_01_01_e.asp.
- ³ *Personal Information Protection and Electronic Documents Act*, S.C. 2000, c. 5
- ⁴ There is a varied literature touching on values issues; e.g. Cohen, Steven. *A Strategic Framework for Devolving Responsibility And Function from Government to the Private Sector*, Public Administration Review 61(4) p. 432; Solove, Daniel *Conceptualizing Privacy*. California Law Review, Jul 2002, 90(4), p1088, 68p.; Stahl, Bernd Carsten *Privacy and Security as Ideology..* IEEE Technology & Society Magazine, 2007 26(1) p35 Westin, Alan F *Social and Political Dimensions of Privacy*. Journal of Social Issues, 59(2), p431; Bennett, Colin & Charles Raab, “The Governance of Privacy Policy Instruments in Global Perspective”, MIT Press, 2006.
- ⁵ The theme that self-enforcing rules implicit in software code dominate written laws or policy is developed in the popular work of Lawrence Lessig, cf. “Code and other Laws of Cyberspace” and “Code v 2”, <http://codev2.cc/>
- ⁶ For example, Public Works and Government Services Canada, Standard Acquisition Clauses and Conditions, online: <http://sacc.tpsgc.gc.ca/sacc/query.do?lang=en&id=K9035D&date=1998/11/23&eid=12>
- ⁷ *Audit Report of the Privacy Commissioner of Canada: Assessing the Privacy Impacts of Programs, Plans, and Policies*, October 2007. online: http://www.privcom.gc.ca/information/pub/ar-vr/pia_200710_e.asp.
- ⁸ See section 7 page 33; in particular the *Privacy Impact Assessment Guidelines: A Framework to Manage Privacy Risks*, Treasury Board of Canada Secretariat publication , May, 2002 online: http://www.tbs-sct.gc.ca/pubs_pol/ciopubs/pia-pefr/paipg-pefrld_e.asp
- ⁹ The Secure Channel initiative [online: <http://www.tpsgc-pwgsc.gc.ca/apropos-about/fi-fs/cvcp-sc-eng.html>] is one example.
- ¹⁰ A similar supply list of companies meeting acceptable security standards already exists (the Cyber Protection Supply Arrangement) coordinated by the Communication Security Establishment. <http://www.tpsgc-pwgsc.gc.ca/acquisitions/text/cp/cyberprotection-e.html>
- ¹¹ An intergrated approach is represented by Memorial University’s privacy strategy project, cf. http://www.mun.ca/iapp/strategy/Final_Report.pdf, comments on page 29 in particular.
- ¹² See *Public Sector Outsourcing and Risks to Privacy*, Office of the Information and Privacy Commissioner , Alberta, February 2006, p.32. online: http://www.cr-international.com/2006_Canada_Alberta_Public-Sector_Outsourcing_and_Risks_to_Privacy_February.pdf
- ¹³ Many of these steps are performed in projects, but they may not be consistently applied or recognized.
- ¹⁴ Federal: *Personal Information Protection and Electronic Documents Act*, S.C. 2000, c. 5 (PIPEDA). Alberta: *Personal Information Protection Act*, S.A. 2003, c.P-6.5 (AB PIPA); British Columbia: *Personal Information Protection Act*, S.B.C. 203, c. 63 (BC PIPA); Quebec: *An Act Respecting the Protection of Personal Information in the Private Sector*, R.S.Q., c. P-39.1. Ontario’s health-sector specific *Personal Health Information Protection Act* has also been declared substantially similar, however it covers only health related activity in Ontario.
- ¹⁵ See footnote 14: PIPEDA s. 3; AB PIPA s. 3; BC PIPA s. 2.
- ¹⁶ See the PROS case study, section 8.1, page 3
- ¹⁷ Office of Privacy Commissioner of Canada website at http://www.privcom.gc.ca/bus/index_e.asp
- ¹⁸ PIPEDA, note 3, Principle 4.3.
- ¹⁹ See note 2
- ²⁰ PIPEDA, note 3, s. 4(2)(a).
- ²¹ S. 7(3)(c) , for example, refers to law enforcement
- ²² See note 2 available from http://www.privcom.gc.ca/legislation/02_07_01_01_e.asp.
- ²³ *Privacy Impact Assessment Policy*, Treasury Board Secretariat, May 2002, available from http://www.tbs-sct.gc.ca/pubs_pol/ciopubs/pia-pefr/paip-pefr1_e.asp#Effectivedate.
- ²⁴ PIPEDA, note 3, Principle 4.7.3
- ²⁵ See note 23 and note 8
- ²⁶ Alternatively, perhaps TBS believes the most cautious approach is to assume both pieces of legislation apply.
- ²⁷ Generally speaking, the potential dissonance is that the vendor may characterize their contract as data services, while the agency thinks it is outsourcing the government service.

²⁸ See note 8

²⁹ See note 6

³⁰ See note 12

³¹ *Guidance Document: Taking Privacy into Account Before Making Contracting Decision*, Treasury Board Secretariat, 2006, online: http://www.tbs-sct.gc.ca/pubs_pol/gospubs/TBM_128/gd-do/gd-do01_e.asp

³² Public values might encompass political accountability, social cohesion, user orientation and similar concepts. Cf. Jorgensen, T.B. & Bozeman, B. "Public values lost? Comparing cases on contracting out from Denmark and the United States", *Public Management Review* 4(1) (2002) 63-81.

³³ See note 31, at p.28.

³⁴ <http://www.infoway-inforoute.ca/en/home/home.aspx>; see also Canada Health Infoway *EHRs Blueprint – an interoperable EHR framework*, version 2, March 2006

³⁵ Ontario: *Personal Health Information Protection Act, 2004*, S.O. 2004, c. 3; Alberta: *Health Information Act*, R.S.A. 2000, c. H-5; Manitoba: *Personal Health Information Act*, S.M. 1997, c. 51; Saskatchewan: *Health Information Protection Act*, S.S. 1999, c. H-0.021; Legislation is currently tabled in Newfoundland and Labrador and in British Columbia.

³⁶ Canada Health Infoway *Electronic Health Record Infostructure (EHRi) Privacy and Security Conceptual Architecture*, version 1.1, June 2005; online: <http://knowledge.infoway-inforoute.ca/EHRSRA/doc/EHR-Privacy-Security.pdf>

³⁷ See note 1.

³⁸ Alternative language is also adopted: the Saskatchewan legislation (see note 35) uses the term "trustee".

³⁹ the term "circle of care", has appeared in widespread use for this concept.

⁴⁰ This conception of privacy has been tacitly encouraged by jurisprudence, e.g. Chief Justice Dickson in *R v. Duarte* [1990] 1 S.C.R. 30: "Privacy may be defined as the right of the individual to determine when, how, and to what extent he or she will release personal information."

⁴¹ Recall that in the case of federal agencies, such contractual requirements appear only in policy guidelines, not in the Privacy Act.

⁴² For example, the restrictions on agents of a custodian in s. 17 of the Ontario *Personal Health Information Protection Act, 2004*, S.O. 2004 is essentially a reference to outsourcing.

⁴³ See note 1, part III, section 4.

⁴⁴ Cf. Pritts, J., and Connor, K (2007) *The implementation of E-consent Mechanisms in Three Countries: Canada, England and the Netherlands, a report for the Substance Abuse and Mental Health Services Administration*, U.S. Dept of Health. Online: www.ihcrp.georgetown.edu/pdfs/prittse-consent.ppdf

⁴⁴ *Summary overview of the electronic consent*. Commonwealth Department of Health and Aging (2002)

⁴⁵ This is examined using e-consent as an example in s. 6 of this report.

⁴⁶ Cf. Passenger Protect Fact Sheet, Office of the Privacy Commissioner of Canada, June 2007, online:

http://www.privcom.gc.ca/fs-fi/fs_20070627_e.asp; see also August 9, 2005 news release, online: http://www.privcom.gc.ca/media/nr-c/2005/nr-c_050809_e.asp

⁴⁷ See note 1, Part I.

⁴⁸ *Trust management* is used here in the sense of modeling how people trust each other. There are alternative uses of this term, including little more than authentication and authorization.

⁴⁹ Standard IEC/ISO 17799 "Code of practice for information security management", International Organization for Standardization (2005); IEC/ISO 27799 "Health Informatics - Security management in health using ISO/IEC 27002": online at <http://www.27000.org/iso-27799.htm>

⁵⁰ *Auditor General's report to the House of Commons: Chapter 3: Large Technology Projects*, Nov 2006; online: <http://www.oag-bvg.gc.ca/internet/docs/20061103ce.pdf>

⁵¹ O'Keefe, C.M., Greenfield, P., and Goodchild, A. (2005) "A Decentralised Approach to Electronic Consent and Health Information Access Control." *Journal of Research and Practice in Information Technology*, 37(2), 161-178.; also see note 56

⁵² Clarke, R. (2002) "e-Consent: A Critical Element of Trust in e-Business." In Proceedings of the 15th Bled Electronic Commerce Conference. URL: <http://www.anu.edu.au/people/Roger.Clarke/EC/eConsent.html>; see also note 59.

⁵³ for an effort to generalize DRM style controls to accommodate individual consent mechanisms, see Lee, G, Kim, W., and Kim, D.-k n(2004) "A Novel Method to Support User's Consent in Usage-Control for Stable Trust in E-

- business.*" In ICCSA 2004. Lecture Notes in Computer Science no. 3045. Springer; Berlin. 906-914.
- ⁵⁴ See note 52
- ⁵⁵ See note 51; also Win, K.T. and Fulcher, J.A. (2007) "*Consent Mechanisms for Electronic Health Record Systems: A simple Yet Unresolved Issue.*" Journal of Medical Systems, 31, 91-96.
- ⁵⁶ Pudney, R. (2003) *e-Consent in Consumer Health and Telemedicine.* online: <http://www.pudney.net.au/~phillip/papers/econsent.pdf>, at page 7
- ⁵⁷ URL references are provided in O'Keefe, Greenfield, and Goodchild (2005) and Pudney (2003), see note 51
- ⁵⁸ Notice is posted at <http://www.health.gov.au/internet/main/Publishing.nsf/Content/404Ref.htm>
- ⁵⁹ Coiera, E. and Clarke, R. (2004) "*e-Consent: The Design and Implementation of Consumer Consent Mechanisms in an Electronic Environment.*" Journal of the American Medical Informatics Association, 11(2), 129-140.
- ⁶⁰ Note 56, at page 10
- ⁶¹ Note 56, at page 11.
- ⁶² Reid, J., Cheong, I., Henricksen, M., and Smith, J. (2003) "*A Novel Use of RBAC to Protect Privacy in Distributed Health Care Information Systems.*" In ACISP 2003. Lecture Notes in Computer Science no. 2727. Springer; Berlin. 403-415.
- ⁶³ Nepal, S., Zic, J., Jaccard, F., Kraehenbuehl, G. (2006) "*A Tag-Based Model for Privacy-Preserving Medical Applications.*" In EDBT 2006. Lecture Notes in Computer Science no. 4254. Springer; Berlin. 433-444.
- ⁶⁴ Bergmann, J., Bott, O.J., Pretschner, D.P., and Haux, R. (2007) "*An e-consent-based shared EHR system architecture for integrated healthcare networks.*" International Journal of Medical Information, 76, 130-136.
- ⁶⁵ Braubach, L., Lamesdorf, W., Milosevic, Z., and Pokahr, A. (2005) "*Policy-rich Multi-agent Support for E-health Applications.*" In IFIP 2005. Springer; Berlin. 235-250.
- ⁶⁶ Berghe, C.V. and Schunter, M. (2006) "*Privacy Injector -- Automated Privacy Enforcement Through Aspects.*" In PET 2006. Lecture Notes in Computer Science no. 4258. Springer; Berlin. 99-117 ; see also Padayachee, K. and Eloff, J.H.P. (2006) "*An Aspect-Oriented Implementation of e-Consent to Foster Trust.*" In SAICSIT 2006. ACM International Conference Proceedings Vol. 204. 164-169.
- ⁶⁷ See note 36
- ⁶⁸ Pritts, J. (2007) *The Implementation of E-consent Mechanisms in Three Countries: Canada, England, and the Netherlands.* Online: <http://ihcrp.georgetown.edu/pdfs/prittse-consent.pdf>
- ⁶⁹ *Privacy Impact Assessment Guidelines: A Framework to Manage Privacy Risks*, Treasury Board of Canada Secretariat publication, May, 2002 online: http://www.tbs-sct.gc.ca/pubs_pol/ciopubs/pia-pefr/paipg-pefrld_e.asp
- ⁷⁰ *Guidance Document: Taking Privacy into Account Before Making Contracting Decision*, Treasury Board Secretariat, 2006, online: http://www.tbs-sct.gc.ca/pubs_pol/gospubs/TBM_128/gd-do/gd-do01_e.asp
- ⁷¹ See note 69
- ⁷² See note 70
- ⁷³ See note 6
- ⁷⁴ See note 69 http://www.tbs-sct.gc.ca/pubs_pol/ciopubs/pia-pefr/paipg-pefrld2_e.asp#3; also see note 70 at page 7
- ⁷⁵ *Privacy Impact Assessment Policy*, Treasury Board Secretariat, May 2002, "Project Initiation," online: http://www.tbs-sct.gc.ca/pubs_pol/ciopubs/pia-pefr/paip-pefr1_e.asp
- ⁷⁶ See note 7, sections 1.36, 1.37, 1.57.
- ⁷⁷ See note 7, section 1.127.
- ⁷⁸ See note 75.
- ⁷⁹ See note 7, section 1.57
- ⁸⁰ See note 75, "Policy requirements, 2. Project initiation,"
- ⁸¹ See note 75, "3. Proceeding with a PIA," and "4. Process Overview," also see note 7, section 1.76
- ⁸² See note 75 "Policy requirements 7. Notification"
- ⁸³ See note 75, section 4.
- ⁸⁴ See note 75, section 4; also see note 7, section 1.71.
- ⁸⁵ *A Guide to Preparing Treasury Board Submissions*, Treasury Board Secretariat, 2007, at page 74. Online: http://www.tbs-sct.gc.ca/pubs_pol/opepubs/TBM_162/gptbs-gppct_e.pdf
- ⁸⁶ See note 7, section 1.22
- ⁸⁷ See note 7, section 1.58
- ⁸⁸ The PIA report is available online: http://www.rcmp-grc.gc.ca/pia/pros_e.htm
- ⁸⁹ Industry Canada's announcement of the project in 2004 in online:

-
- <http://www.ic.gc.ca/cmb/welcomeic.nsf/0/85256a5d006b972085256f690056a4a8?OpenDocument>
- ⁹⁰ The PIA for the project is available online: http://www.tpsgc-pwgsc.gc.ca/atip/text/priv_impact_assessment-e.html
- ⁹¹ Announcement of the contract award is available online:
<http://www.sierrasystems.com/PressroomDetail.aspx?id=pressroom&year=2003&newsid=91>
- ⁹² The PIA for the IQT is available online: http://www.rcmp-grc.gc.ca/pia/iqt_e.htm
- ⁹³ Advertising and Marketing Update, McMillan Binch Mendelsohn, July 2006, online:
http://www.mcmbm.com/Upload/Publication/BillC37Update_Canadas-DoNotCallList_0906.pdf
- ⁹⁴ Legislative Summary for Bill 37, Library of Parliament, Feb 2007, online:
http://www.parl.gc.ca/common/bills_ls.asp?Parl=38&Ses=1&ls=c37
- ⁹⁵ Canadian Marketing Association Website, Consumer Information. <http://www.the-cma.org/?WCE=C=32%7CK=S224196>
- ⁹⁶ See note 94
- ⁹⁷ *Telecommunications Act*, S.C. 1993, c. 38 as amended, sections 41.1 to 41.7
- ⁹⁸ See section 4.3.3
- ⁹⁹ *Privacy Matters: The Federal Strategy to Address Concerns About the USA PATRIOT Act and Transborder Data Flows*, Treasury Board Secretariat, 2006, online: http://www.tbs-sct.gc.ca/pubs_pol/gospubs/TBM_128/pm-prp/pm-prp07_e.asp
- ¹⁰⁰ Information Notice - Access to Information and Privacy - Guidelines for Privacy breaches; and Explanatory Notes to Privacy Protection Checklist, Treasury Board Secretariat, 2007, online: <http://www.tbs-sct.gc.ca/atip-airp/in-ai/in-ai2007/2007-02-in-ai-eng.asp>. Also see note 31, appendix B.
- ¹⁰¹ Canadian Association of Financial Institutions in Insurance, website news item, august 2006 online:
http://www.cafii.com/whatsnew/whatsnew_august_1_2006.html
- ¹⁰² CRTC Interconnection Steering Committee Report to the CRTC - Non-Consensus Report: TIF Non-Consensus Items, July 2006, sections 47-48, online: http://www.crtc.gc.ca/cisc/eng/CISF4h_1.htm
- ¹⁰³ MERX is an online system for managing public tenders used by the GoC.
- ¹⁰⁴ Senior Manager-Telemarketing Regulations - CRTC
- ¹⁰⁵ See note 90
- ¹⁰⁶ The PCI Security Standards Council publishes its standards and license agreement online:
https://www.pcisecuritystandards.org/tech/download_the_pci_dss.htm