Government Information Sharing

Is Data Going Out of the Silos, Into the Mines?

Principal Authors:
Stephanie Perrin, Jennifer Barrigar and Robert Gellman
Digital Discretion Inc.

January 2015

An Independent Research Report Commissioned by the
Office of the Information and Privacy Commissioner of Alberta

Digital Discretion Inc.
P.O. Box 183, 155 MacFarlane Street
Pakenham, ON, K0A2X0
www.digitaldiscretion.ca
stephanie@digitaldiscretion.ca

Table of Contents

Executive Summary

Introduction

This research explores government sharing of personal information across ministries and services, or with the private sector for the provision of services. The report reviews material from many sources on government data sharing activities with a particular focus on privacy. There is no explicit or consensus framework for assessing or evaluating data sharing. While data sharing goes on in Canada it does so under the rather antique framework of public sector laws that ill equip privacy practitioners to deal with data mining realities of 2014. Meanwhile, there is ongoing discussion how or whether privacy expectations need adjustment to reflect the new reality of "big data".

Data sharing includes data matching, joint access to repositories of data, file duplication, and any method of data access that enables more than one agency or organization to use personal data. Data sharing results in personal data moving out of traditional data silos and being used in new ways, by different agencies, or for new or different purposes.

Many factors have been influential in preventing or limiting large scale data sharing, or "joined-up government" initiatives. Large systems are sometimes just too hard to run, let alone merge with other large systems in other organizations. This can be especially true when government agencies operate the systems. Globally and at the federal level in Canada, some spectacular government information technology (IT) failures caused bureaucrats to be cautious. Some agencies zealously protect their "turf" and their data, fearing loss of influence or budgets. A relatively new concern relates to financial and reputational risk in the event of data breach.

The goal of this report is to provide a broad survey of the topic, potential frameworks for analysis, and a critical examination of some of the actions taken to protect privacy.

The current situation involves barriers to rather old problems, such as a simple data match, being enforced, while new initiatives, such as data analytics and the use of private sector databases and profiling tools, proceed without adequate public discussion. This state of affairs is especially troublesome for those who approach data sharing with privacy concerns.

For this report, the authors review a broad range of data sharing initiatives from the last several decades.

The primary focus is on privacy. It is important to remember, however, that when a data sharing initiative fails the failure typically has many causes, and seldom is privacy the principal one. A "loss of privacy" is often the label pasted on what amounts to a loss of trust in government.

The goal of this report is to provide a broad survey of the topic, potential frameworks for analysis, and a critical examination of some of the actions taken to protect privacy.

Silos and Their Discontents

Around 2000, the rallying cry "let's break down the silos" started to be heard. The goal was to make greater use of information stored in its own sealed column – or silo – within an agency, isolated from the rest of the government and the rest of the world. In Canada, this coincided with attempts to cut administrative costs by amalgamating services.

The advent of computing power came in three waves, with large single purpose mainframes in the 1960s and 1970s, desktop computing in the 1980s, and networked computing in the 1990s. Given this rapid change in the way services were provided, it is not surprising that public servants at all levels often lacked the insight necessary to determine fair information practices with respect to personal information.

In 1973, a United States (U.S.) federal advisory committee issued a highly influential report that proposed Fair Information Practices (FIPs) as core principles for protecting privacy of personal information.

One of the committee's five FIPs sought to limit uses and disclosures, in particular preventing information collected for one purpose from being used for another purpose without consent.

The objective of limiting the use of personal information to the original purpose is at the heart of the struggle over data silos. When can data collected for one program be used for another program? Who decides what the purpose of collection is? Where does individual consent fit in? Similar issues arose in Canada with the federal *Privacy Act.* The law permitted the use of information within an agency for a "use consistent" with the purpose of the collection, and soon the number of consistent uses (or purposes as it came to be interpreted) mushroomed.

During the early 1990s in Canada, the federal Committee for Administrative Renewal in Services looked at the forces that prevented information sharing, expecting to find the 1982 *Privacy Act* as the deterrent. In fact, the barriers came from elsewhere. Privacy legislation was not the only or even the principal barrier.

Several factors combine to make information sharing in Canada more complex, particularly as compared to other parliamentary democracies like the U.K.

- Services to citizens are inherently split between federal and provincial levels.
- Transborder dataflow to the U.S. is both a reality and a bogeyman. When data is not in Canada it is harder to enforce Canadian law, notably privacy law.
- The opening up of trade in government procurement means that any big systems are accessible to bidders from foreign states.

Benefits of Breaking Down the Silos

The benefits of data sharing do not solely accrue to the governments or organizations that collect, use and disclose the information. There are definitely benefits to the citizenry. Anyone who has ever changed provinces with children in school and elderly parents in need of healthcare would fight for one-stop shopping, and single source address change. Other potential benefits include: convenience for the citizen; better program delivery through a comprehensive or clustered approach; automatic

entitlement to programs; better risk management and cost control; efficiency through more effective use of data; and better information dissemination and training.

Risks of Data Centralization, Distributed Shared Access, and Data Mining

Fears of giant databases have been around since the 1960s, and specific risks or worries include:

- use of data for purposes unrelated to the purpose for which the data was collected;
- loss of control of data by agencies;
- inability to correct errors as data travels;
- outdated/incomplete records (e.g., criminal history records without dispositions);
- conflicting time periods resulting in incorrect linkages and inferences;
- decisions made using unrelated, inaccurate data without the knowledge of the citizen;
- hostile users (i.e., the citizen may not know which organization ultimately holds and uses the data, and there may be no trust relationship);
- profiling and the possibility of discrimination (e.g., potential *Canadian Charter of Rights and Freedoms* issues);
- lack of accountability;
- absence of enforceable rights (e.g., due process);
- legal complexity because of sharing among federal/provincial/territorial (FPT) agencies; and
- the consequences of greater transparency.

These risks point to a glaring need for more informed public discourse on the topic of data sharing and data analytics.

Data Mining and Big Data

Data sharing has now morphed into data mining, and much rhetoric exists today about the benefits of "big data". Many terms appear in the popular and IT media about the topic of data mining, including big data, risk profiling, data analytics, predictive analytics, regression analysis, knowledge discovery, and so on. Unfortunately, many of the touted benefits of big data that includes personal information are, to a privacy advocate, a worst nightmare. There is healthy skepticism elsewhere in the privacy world about whether privacy needs to make accommodations to so-called big data.

Data sharing has now morphed into data mining, and much rhetoric exists today about the benefits of "big data".

Privacy, the Charter, and Information Sharing

The *Canadian Charter of Rights and Freedoms* (Charter) protects the fundamental rights and freedoms of persons against state action. The Charter does not contain the word "privacy" or a freestanding right to privacy. Yet privacy interests have been recognized as being foundational to other protections granted by the Charter. Section 7 of the Charter states that, "[e]veryone has the right to life, liberty and security of the person and the right not to be deprived thereof except in accordance with the principles of fundamental justice." The liberty interest is grounded in privacy rights, especially in relation to an individual's control of her body and of her personal information.

The other – and more commonly invoked with regard to privacy – Charter section at issue is section 8, which grants a right to be free from unreasonable search and seizure. Section 8 protects people and not places; in particular, it protects a biographical core of personal information which individuals in a free and democratic society would wish to maintain and control from dissemination to the state.

Case Studies and Analysis

For this report, the researchers selected a broad range of data sharing initiatives from the last several decades to review and analyze. A template for examining initiatives was developed, dubbed the "W5 and HOW" approach, which sets out the following:

- WHO: Who are the agencies or entities that share or match information? Who are the individuals whose personal information is shared? Who pays the transactional costs? Who is responsible for the contracts, the personal data protection, the oversight, etc.? Who performs the work?
- WHAT: What personal information is shared or transmitted, for which programs, and what benefits result from the practices?
- WHEN: When will the sharing take place, or has it already started? Is this an extension to an existing practice, and if so does it alter the substance, purpose, or nature of current practices? Are there sunset clauses to terminate the exercise?
- WHERE: Where is the data sharing taking place? Where is the data processed and stored? Where are the systems and software located? Is there outsourcing? Are "cloud services" involved? Are borders crossed? In what jurisdiction does the processing take place?
- WHY: Why is the sharing needed? What are the benefits? What are the costs?
- HOW: How are software, technology, and databases used to share or transfer data? Is the activity characterized as a data match, a simple permission to access data between staff of different agencies, a duplication of databases, or a data mining (data analytics) activity? Is a data warehouse involved?

This framework is used to examine each case study, although not all questions necessarily have answers. Using these basic principles of analysis, 12 data sharing initiatives from seven different jurisdictions were examined. Each example includes conclusions, some of which are highlighted in this summary.

1. Australia: The Australia Card

The attempts of several Australian governments to introduce identity cards are famous in the lore of national identity cards. The Australia Card had actually already gone into production in 1987 when it was withdrawn based on a public uproar, with opposition to the card coming from all sides – right, centre, and left. The idea resurfaced in later years, but it failed each time.

- Whether a good idea or not, the Australia Card was not developed with adequate participation by all stakeholders or the public.
- The card affected too many constituencies at once, which generated widespread opposition.
- High profile data sharing activities that directly affect individual citizens often receive more attention than data sharing that occurs quietly between government departments

out of the direct sight of data subjects, but which may have equally significant privacy concerns.

2. Australia: Centrelink Master Program

Centrelink was originally setup in Australia under legislation in 1997 with the mandate to provide services to government programs that provided services, benefits, programs or facilities. As the system evolved over time, it did not create one central database but supported separate customer databases held by each individual agency with data sharing based on a consent model. Different programs eventually became integrated under a single government department that serviced customers with a single telephone number and website.

- The Centrelink project is widely seen as a success, in part because it provided services to individuals, whereas the Australia Card was disembodied from benefits to individuals, except for the notable exception of single point address change.
- Centrelink provided individuals with some degree of control and choice, allowing those with specific privacy concerns to tailor their experience. This may have addressed, to some extent, the concerns of those who might otherwise have been most vocal about privacy.
- Over time, Centrelink built up a large number of users. Providing service and convenience can prompt citizens to ignore privacy issues, as has been seen with any number of private sector services. This does not mean that privacy is a dead issue, but it may reflect the way risk analysis is calibrated by the average individual.

3. Canada Provincial: BC Services Card

In 2011, the Government of British Columbia (B.C.) established a multi-year, multi-phase project intended to develop a smartcard credential and associated identity information management system; implement the cards and put them into the hands of users; and then build a system where access to various government services is available using the cards and identity information services.

B.C. created a card that combines the driver's licence and the health card. The BC Services Card is government-issued identification that allows its holders to provide authentication of their identities and access provincial services. The card will provide a central point of access to more services as time goes on. Privacy remains protected because individual silos of information are not aggregated.

- It is too early to offer firm conclusions about the impact of public and privacy concerns on the BC Services Card, but relevant points of view are being heard in the decision-making process.
- Government efforts at public consultations expanded in response to criticism.
- The Information and Privacy Commissioner of B.C. had an early opportunity to review the project and provided useful advice that the government responded to.

4. Canada and the Provinces: Single Sign-On and E-Services

The Treasury Board Secretariat of Canada (TBS) started the Lac Carling meetings in 1996 by bringing together officials from all jurisdictions, as well as private sector IT companies, in an effort to kick-start the desired transformation of government e-services. Given that the Lac Carling

discussions have gone on for so long, and are really the forum for FPT discussions of "joined-up government," it is interesting that progress on joint efforts appears to be slow.

- The lack of transparency for the Lac Carling discussions is in sharp contrast to other countries involved in e-government.
- The initiative started with a focus on authenticating individuals for centralized service and data sharing. The fact that this forum appears to have become less active in the area of identification authentication may indicate the difficulty of the task.
- Privacy has never been a key focus of this conference, although the topic was recognized as a potential barrier to data sharing, and a working group was struck to study the issue.

5. Canada: E311 Data Matching

The program is an illustration of a classic data match, and is interesting because the Privacy Commissioner of Canada fought it in the Supreme Court of Canada (SCC). E311 Customs Declaration Cards collected information from travelers into Canada for regulation of goods importation. The data was later matched with the Employment Insurance files to look for claimants not entitled to benefits while they were absent from Canada. There were agreements between the relevant departments about the use of the data.

The Privacy Commissioner expressed concerns about the project, in particular about lack of proportionality, unnecessary sharing, lack of transparency, and the absence of a written agreement. The Privacy Commissioner took the matter to the Federal Court, the Federal Court of Appeal, and the SCC, but eventually lost the case. Since then, the information sharing has been codified in regulation and policy.

- This is a good example of a case where an organization, wishing to do a data match, availed itself of the regulatory authority to do the match without getting additional parliamentary authority, consulting with stakeholders, publicizing its plans, or any of the other processes that might be expected in new potentially invasive data sharing exercises.
- The actual savings reported from the data match may have had a bearing in the case. Wholesale perusal of the travel records of Canadians with no proof of benefits to the match might have been a more difficult case to argue.
- At one level, the Privacy Commissioner's decision to take the matter to court was not successful. The choice of tactics makes a difference, and going to court is definitely playing for "higher stakes". However, win or lose, the case generated a great deal of necessary discourse on the issue of data matching, and may have accelerated the promulgation of other remedies, such as privacy impact assessments (PIAs).

6. Global: The WHOIS Directory

ICANN, a private organization, is a key player in international Internet governance. ICANN sets rules for the collection, use, and disclosure in a public directory of information on domain name holders, with many stakeholders wanting access to the information. Finding the right balance for permissible purposes of the information is complex, with many governmental and non-governmental organizations, commercial and non-commercial interests, and public interest players, and many conflicting goals.

- The ICANN domain registration problem is complex with many different players and with government agencies potentially on different sides from each other. Different parts of the same government can have different views.
- The clash between Internet governance and data protection controls is yet to take place, and the results are hard to predict.
- ICANN is an example of a new form of international governance structure, the "multi-stakeholder model".
- Transparency is necessary but not sufficient for privacy representation.

7. U.K.: Joined-Up Government

For many years, the U.K. government has tried to do "joined-up government", or provide the government with extensive data sharing powers and technical ability for social and other services. The lengthy history shows much complexity, designs for centralized databases, and data sharing across traditional provider and departmental boundaries, major and expensive IT failures, and extensive reviews and reports from inside government and outside.

- Central databases may be more prevalent in countries where power and administration are centralized and not shared with provincial governments.
- While there was a first wave of enthusiasm for joined-up government after/during the dotcom boom, enthusiasm waned as governments realized how complex the projects are. Failures were numerous, but the desire to reduce cost and predict risk continues to drive data sharing initiatives.
- Privacy and human rights concerns, including intrusion and discrimination, are serious impediments to joined-up government, although they are far from the only impediments.
- In the early attempts at joined-up government, funded U.K. advocacy groups exposed issues and mounted campaigns for change.

8. U.K.: Children's Services

The U.K. government shifted from a child protection model of social services, responsive to reports of abuse, to a "prevention" model. Prevention models use risk factors to identify children likely to be at risk in order to establish surveillance, and involve them in activities less likely to lead to crime and underachievement. A highly publicized death of a child contributed to the change.

The effort involved linking numerous and diverse databases maintained by multiple agencies for different purposes. Reports and academic analyses of the effort raised many legal, technical, privacy, ethical, and other concerns about the linkage.

- Tragic events can propel social policy in ways that may skew the emphasis on procedures. As is clear from the U.K. example, horror stories can cut both ways.
- Intervention, whether to detect fraud, child abuse, or disease, must be done by humans who evaluate the data and determine that scarce resources should be spent on this or that case. A system that produces more "hits" than a staff or budget can review and investigate may create more demands for accountability.
- Penalties or bad press for under-reporting can drive scope creep and over-reporting.
- Academics and civil society played a key role in public discussions.

9. U.S.: Internal Revenue Service Sharing Tax Data with States

The principal function of the Internal Revenue Service (IRS) in the U.S. is the collection of income taxes. IRS shares tax information with federal, state, and local agencies for purposes specified by law. IRS requires users of tax returns to meet strict security requirements based on widely accepted standards.

- When the stakes – be it personal data or agency turf – are high enough and the resources are available, it is possible to develop a comprehensive program to oversee the confidentiality of shared information.
- Requiring those who want access to personal information to sign agreements establishing the terms of data use and data security will work when the interest in data sharing is high.
- With respect to computer security requirements, it is not necessary to reinvent the wheel, but standards established by respected external organizations can be referenced and used.
- The IRS had sufficient incentive to protect its turf and its data without outside pressure.

10. U.S.: *Computer Matching and Privacy Protection Act*

Computer matching began in the U.S. as an administrative activity and policy controversy in the late 1970s. An initial legal question was whether it was compatible with the purpose of one set of records to use the records for an unrelated program. Political and budgetary pressures overcame legal and policy objections. Privacy eventually staged a comeback with the *Computer Matching and Privacy Protection Act* in 1988. The law's procedural controls were not successful due to absence of oversight and technological developments. The law's due process provisions were more successful.

- The absence (or presence) of a high level data protection authority can contribute to the success or failure of privacy controls for computer matching.
- Providing due process for individuals may be more important than providing privacy controls. Due process and privacy are not, however, mutually exclusive.
- Privacy controls based on specific technological implementations will become outdated if they are not adjusted to later development.

11. U.S.: Department of Homeland Security Information Sharing Strategy

The U.S. Department of Homeland Security (DHS) is a federal agency that is a complex amalgam of agencies, missions, and programs. Data sharing is a major activity, managed through a high level strategy. The objective of the strategy is the establishment of a DHS Information Sharing Environment that allows internal sharing of critical information. Privacy is an important element of the strategy. Elements of the DHS strategy of broader interest include:

- a formal data sharing strategy rather than a series of uncoordinated policies;
- a high-level data sharing governance board rather than ad hoc or low-level data sharing decision making;
- addressing privacy early in planning rather than never or when it may be too late;
- use of information sharing agreements rather than informal arrangements;
- audit logs rather than no method for ensuring compliance and adjusting policies; and
- the use of technology and data tagging to control use and disclosure of personal information in a more granular way rather than role based access controls.

12. Denmark: E-Government Services

Denmark has been a leader in e-government for a number of years. It has a high level of broadband services and a high level of Internet use among the population. There are three components to its e-government system: a citizen portal, where citizens can access all their transactions with government; a secure email and archive system, which were set up through a public-private partnership and which allows communication with government and private sector actors; and a secure digital signature system which operates across numerous platforms.

- Denmark successfully transitioned to e-services for the citizen.
- There is little focus on privacy as an issue, but there is transparency of data sharing.

Citizen Expectations and Data Sharing

What are citizen expectations with respect to their data? When is data sharing acceptable and when is it objectionable? Do citizen expectations coincide with the "reasonable expectations of privacy" standard assessed by the courts? If not, what should be done? In some ways, one of the great mysteries of privacy is why one event, incident, or policy elicits overwhelming opposition from the public while others that may be similar or more intrusive are ignored.

In some ways, one of the great mysteries of privacy is why one event, incident, or policy elicits overwhelming opposition from the public while they ignore another that may be similar or more intrusive.

A successful information sharing project not only increases efficiency but better serves the needs and expectations of its users and its data subjects. Accordingly, expectations are a relevant and important consideration. The problem here is that detailing or mapping the extent of further data sharing is a massive problem partly because existing systems of database linkage are not well explained. It is hard to keep monitors of data sharing activities up-to-date.

Examining Risk in Data Sharing Projects and Proposals

Based on the analysis of the various data sharing initiatives and strategies, the key risks and mitigations identified in data sharing can be clustered around the following themes.

Legal Authority

- Organizations require the legal authority to collect, use, and disclose or share the data.
- Separate organizations require contractual authority, sharing agreements, or in the case of separate nations, a treaty or other authority to share data.
- All authority relied upon for data sharing, including contracts with the private sector, must be reviewed for constitutional correctness and legal compliance.
- Personal data should be maintained in a way that maximizes the application and enforceability of privacy law.
- Independent oversight of all authorities is essential.

Potential mitigations: new regulations or new legislation; regulatory impact assessment; charters of data sharing partners; contracts for major activities reviewed by data commissioners; and public and civil society comment during planning, contracting, and implementation stages of data sharing

Procedural Fairness

- Public acceptance depends on many factors, with legal and constitutional compliance being only some of them. More generally, a project must be seen as fair to the citizen in order to be accepted.
- Assessment of constitutional risk is one tool that is sometimes used to assess fairness, but too often that assessment results in a review of case law rather than a thoughtful exploration of whether in fact the proposal meets "the smell test".
- Fairness often requires a political and an ethical judgment and not just a legal one.
- Where individual interests are at risk, formal due process procedures are essential.

Potential mitigations: focus groups of affected citizens; participation by privacy commissioners; participation of constitutional scholars and civil society on working groups; an internal ombudsman or privacy officer for a data sharing initiative; and availability of information about fundamental rights.

Financial Risk

- The existing record of failed government IT projects suggests strongly that many major hardware or software projects will never reach implementation. No one ever thinks that their project will fail, but history demonstrates otherwise.
- Inadequate funding, whether from overly optimistic vendor estimates, projected program savings, or timelines for completion, is a significant risk in government IT projects.
- Cutbacks in spending can impact ongoing projects, and make risk mitigations inoperative. The possibility exists for failing projects and inadequate privacy.

Potential mitigations: public consultations and independent second opinions for funding estimates; program managers constantly ensuring that privacy risk mitigations are still in place; regular reporting to privacy commissioners during development and initial implementation; and funding for privacy mitigations as a percentage of overall spending.

Organizational Commitment to Privacy

- Who owns the privacy problem? In a mature organization that realizes privacy is fundamental, the organization takes responsibility for having a mature privacy program, including competent senior officers in charge of it, training, PIA review, audit, etc.
- If privacy as a policy issue has become a risk, those involved may not challenge the risks or may understate the risks.
- New technologies such as data mining and cloud services raise complex privacy risks, requiring significant expertise and dedication to sound public policy.
- Public concern about privacy can be both wide and deep, but it is often unpredictable. A lack of commitment allows organizations to make gestures to privacy, and focus on other political and policy issues that are also important to Canadians.

Potential mitigations: leadership to achieve organizational commitment; a privacy commissioner can sometimes nudge senior officials in the right way at the right time; ownership of privacy as an issue has to reach the middle managers for the culture to change; media attention to privacy issues; public interest groups can hold government accountable over privacy; and a crisis intervention plan for dealing with disasters.

Security Management

- Security protocols using generally accepted standards and best practices need to become requirements for all projects. Reinventing the security wheel should rarely be needed.
- Regular reporting on security audits should be included in project management plans.
- Audit logs for data use and disclosure provide critical checks.
- Training is essential for all staff involved in the project.
- Sanctions for staff who do not follow security procedures need to be significant, administered fairly, and visible as appropriate.

Potential mitigations: external audit of security measures, procedures and protocols, including management of audit logs; data analytics of audit logs; whistleblower support; and guidelines for acceptable government or private sector security standards by a privacy commissioner.

Project Scope Creep

- Once a new use of data is found, there is a risk that it will lead to new uses, demands for more data, and more data sharing.
- Costs of running data analytics programs or data warehouses tend to favour scope creep, as high volumes of data and repeat use of software are needed to justify costs.
- Once barriers to sharing with one agency or partner are dropped, there is a risk that the organization will not be able to refuse sharing with another agency.

Potential mitigations: selecting the right partners who have inherent concerns about misuse of their data; right-sizing data collection to recognize bureaucratic and budget limits; and independent review by a privacy commissioner identifying and raising questions about new data sharing activities.

Data Mining and Data Elements

- Data mining is the latest bright shiny toy. It is not clear that it is always useful in the government services context, but IT departments want it because it is state of the art.
- Predictive analytics have uses, but less so in social services and every other sector of public service where individuals are entitled to service without discrimination.
- Big data is a concept that can be directly contrary to the fundamentals of privacy, namely scope and volume limitation, and restriction to stated purposes.
- Data elements need to be assessed for relevance and accuracy.
- Data protection does not lose relevance because of new technology or new applications.
- U.S. companies may be leaders in data analytics and data collection, but some may be laggards in data protection rights.

Potential mitigations: comprehensive regulatory impact assessments for predictive analytics; cost-benefit analyses; sunset provisions; public education; and collective work by privacy commissioners.

Transborder Legal Demands and Jurisdiction

- The availability of data for use in foreign courts is currently under litigation in several jurisdictions. There is no certainty as to whether individuals can enforce their rights when the data is held outside the country.

Potential mitigations: TBS guidance on contracting; keeping personal data within the jurisdiction where it is used; and cooperation between privacy commissioners and legal authorities.

Group Privacy

Group privacy is not currently well understood in data protection, nor is there much research on how best to protect it under existing law. Human rights law may have relevance in this context.

- Some groups may experience invasion of privacy or discrimination to a greater extent in data sharing activities, depending on the situation.
- Some groups may be more resistant to data disclosure or data use because of their history, religion, or perception of invasion of group privacy.
- Data mining algorithms may casually create groups or profiles that may have persistence and that may stigmatize group members in major ways.

Potential mitigations: review of data analytics programs through targeted PIAs; consultation with affected groups; and greater awareness of group privacy concerns.

Research Ethics

Identifiable personal data used for statistical analysis when "joined-up" should be subject to research ethics review because of sensitivity or the possibility of re-identification.

Potential mitigations: greater use of research review boards; review of some research protocols by privacy commissioners; and insistence on data use agreements to prevent re-identification and to provide accountability.

Public Relations and Communications

- Insufficient communications and transparency about the data sharing project may create suspicion in various stakeholder groups.
- Insufficient awareness of technology capability, data management practices, and current data holdings, may precipitate an over-reaction to a modest, lawful data sharing practice.
- There is a risk that individuals' expectations with respect to the protection of their personal data could be raised to unsupportable levels.
- There is a risk that any potential communications will be regarded negatively by organizations engaged in data sharing (i.e. a belief that open discussion of privacy risks may trigger a negative reaction, threatening an initiative).
-
- There is a risk of losing control of messaging, especially with the advent of social media.

Potential mitigations: greater transparency; stakeholder meetings; and town hall meetings with citizens.

The elements described above are broad categories. For each one there could be a more complete breakdown of risk elements and mitigations, but this suffices to give a background for discussion of strategies and approaches to evaluating, commenting on, and intervening effectively on data sharing initiatives.

Conclusion

There is no one course to chart with respect to data sharing. This report has attempted to sketch out where the issues are the same as they have always been since the first data collections on computers, and where they are different because of powerful new technologies. Similarly, some risks are about the same, and others have increased significantly. Trust in governments has always been somewhat fragile – with or without technology – but the risks of identity theft, social exclusion, and reputational damage may well have gone up because of today's big data. Because some risks have increased significantly, it is important that remedial action takes place. Fortunately, those risks are owned by many stakeholders, so that information commissioners can play a broker role in raising awareness, issuing advice, promoting higher standards, and persuading all stakeholders to take privacy and the respect for the dignity and autonomy of each individual seriously.

All Canadians want the benefits of electronic government services, and reduction of administrative burdens. Some of us still want our privacy and autonomy too. We should go into discussions of data sharing fully informed of the risks and possible strategies to mitigate those risks. It is hoped that this report makes a useful contribution to that vital discourse.

I. Introduction

This research explores government sharing of personal information across ministries and services, or with the private sector, for the provision of services with a particular focus on privacy. It is a research paper that reviews material from many sources on government data sharing activities. A range of examples were selected, both domestic and international, in order to illuminate different aspects of the risks, experiences, best practices, and evaluations of data sharing initiatives.

It is worth noting that here in Canada and in other democratic western states data sharing has been discussed for many years. However, there remains no explicit or consensus framework for assessing or evaluating data sharing. While data sharing goes on in Canada, it does so under the same, rather antique framework of public sector laws that ill equip privacy practitioners to deal with data mining realities of 2014.

Meanwhile internationally, there is ongoing discussion about how or whether privacy expectations and principles need to be adjusted to reflect the new reality of "big data". While so-called big data is peripheral to this study of data sharing, calls for changes in legislation to provide more flexibility for enhanced collection, use, and disclosure of data are not. Recently, the Article 29 Data Protection Working Party of the European Commission responded to this trend by releasing a new opinion on big data, affirming the relevance of existing data protection law: "However, at this stage, it has no reason to believe that the EU data protection principles, as they are currently enshrined in Directive 95/46/EC, are no longer valid and appropriate for the development of big data, subject to further improvements to make them more effective in practice. It also needs to be clear that the rules and principles are applicable to all processing operations, starting with collection in order to ensure a high level of data protection."[1]

Additionally and perhaps related to the long-standing perception that data sharing means a loss of privacy, there seems to be a reticence to engage in a fulsome discussion of what data sharing actually means today. One possible reason for the lack of discussion is fear of a public backlash from the perceived breaking down of barriers that protect privacy.

A word on definitions: the word "sharing" does not usually appear in privacy legislation. It is a word that is often used because it sounds friendlier than "disclosure" or "use", although those words are usually more precise. The term "sharing" can be less clear and less precise about location and method, just as references to "cloud services" can be vague about data location, transfer, control, and application of law. References to data sharing in this paper include data matching, joint access to repositories of data, file duplication, and any method of data access that enables more than one agency or organization to use personal data. Data sharing results in personal data moving out of traditional data silos and being used in new ways, by different agencies, or for new or different purposes.

[1] http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp221_en.pdf

Many factors have been influential in preventing or limiting large scale data sharing, or "joined-up government" initiatives. Large systems are sometimes just too hard to run, let alone merge with other large systems in other organizations. This can be especially true when government agencies operate the systems. Globally and at the federal level in Canada, some spectacular government IT failures caused bureaucrats to be cautious[2], particularly in periods of fiscal restraint such as experienced in Canada for the past 20 years. Existing systems have barriers to integration including the hardware platform, operating system, and data formats. It may be impossible to achieve an acceptable rate of data matching because of missing data elements or unreliability of key data fields. At times, government institutions do not have sufficient trust in one another to sustain a data sharing initiative. Some agencies zealously protect their "turf" and their data, fearing loss of influence or budgets. Costs and division of responsibilities present other obstacles. A relatively new concern relating to financial and reputational risk in the event of data breach increases the consequences of partnerships, even in the public sector.

Transparency surrounding initiatives such as "single window" service delivery has long been an issue. Sometimes, as has been the case with the federal-provincial discussions on identity management in Canada, reticence to be fully transparent may stem from the delicacy of interprovincial discussions. This is equally true of international data sharing initiatives. Leading examples here come from anti-terrorism initiatives after 9/11, notably those relating to Passenger Name Records (PNR) and no-fly lists. The lack of clear exposition of initiatives on the part of governments makes it difficult to find consistent, detailed information about data sharing initiatives.

The current situation involves barriers to rather old problems, such as a simple data match, being enforced, while new initiatives, such as data analytics and the use of private sector databases and profiling tools, proceed without adequate public discussion.

The current situation involves barriers to rather old problems, such as a simple data match, being enforced, while new initiatives, such as data analytics and the use of private sector databases and profiling tools, proceed without adequate public discussion. This state of affairs is especially troublesome for those who approach data sharing with privacy concerns.

---

[2] Britain outsourced its Inland Revenue Service back in the 1990s, to EDS, and ran into embarrassing issues when they wished to cancel the contract. It appeared that EDS was in too deep to leave. http://www.computerweekly.com/feature/Inland-Revenue-EDS-Divorce-Impossible. However, the contract was granted to Cap Gemini, after some two years of evaluating tender proposals. Here in Canada, HRSDC has attempted to update its legacy systems, but have been unable to do so despite warnings from the Auditor General in the 2010 Spring Report (http://www.oag-bvg.gc.ca/internet/English/parl_oag_201004_01_e_33714.html) that critical systems were on the verge of collapse. This was one of the reasons for the creation of Shared Services, to provide central expertise and more rigid control of IT projects. http://www.ssc-spc.gc.ca/pages/bckgrnd-cntxt-eng.html. There are similar examples in other jurisdictions as well.

For this report, a broad range of data sharing initiatives from the last several decades were selected for review. A template for examining initiatives was developed, dubbed the "W5 and HOW" approach, which sets out the following questions:

- WHO: Who are the agencies or entities that share or match information? Who are the individuals whose personal information is shared? Who pays the transactional costs? Who is responsible for the contracts, the personal data protection, the oversight, etc.? Who performs the work?
- WHAT: What personal information is shared or transmitted, for which programs, and what benefits result from the practices?
- WHEN: When will the sharing take place, or has it already started? Is this an extension to an existing practice, and if so does it alter the substance, purpose, or nature of current practices? Are there sunset clauses to terminate the exercise?
- WHERE: Where is the data sharing taking place? Where is the data processed and stored? Where are the systems and software located? Is there outsourcing? Are "cloud services" involved? Are borders crossed? In what jurisdiction does the processing take place?
- WHY: Why is the sharing needed? What are the benefits? What are the costs?
- HOW: How are software, technology, and databases used to share or transfer data? Is the activity characterized as a data match, a simple permission to access data between staff of different agencies, a duplication of databases, or a data mining (data analytics) activity? Is a data warehouse involved?

This framework is used to examine each case study, although not all questions necessarily have answers.

First, the primary focus of examining data sharing initiatives is on privacy. It is important to remember, however, that when a data sharing initiative fails the failure typically has many causes, and seldom is privacy the principal one.

Second, individuals, businesses, and governments are increasingly anxious about surveillance, most recently in the wake of the Snowden revelations about surveillance by the United States (U.S.) National Security Agency (NSA). The documents released concerning intelligence activities appear to have significantly undermined the trust placed in some of the information technology (IT) companies with whom they do business, to say nothing of governments.[3] Several examples of data sharing activities described in the paper failed due to the impact of media reports. The risk may be greater today that publicity will cause a project to be shut down in the wake of negative press regarding surveillance.

Third, the authors do not wish to imply that the lack of trust in government is either new or attributable only to recent revelations. One of the earliest examples is the Australia card in 1988, which exhibited a lack of trust in government. A loss of trust in government is one of the major

[3] See PC Magazine for a (February 2014) summary of its ten most alarming Snowden revelations. http://www.pcmag.com/article2/0,2817,2453128,00.asp. The final item on the list is that "Microsoft, Google, Yahoo, Facebook, PalTalk, YouTube, Skype, AOL, and Apple were all named in the PRISM documents and struggled with how to talk to the public about it because of gag orders."

casualties of some government initiatives, and it is often a root cause of a lack of uptake of e-government services[4]. Loss of trust is detrimental to democracy and to the values that Canadians cherish. Because "privacy" is often somewhat loosely defined in the minds of the public, a "loss of privacy" is often the label pasted on what amounts to a loss of trust in government and to fears about a new distribution of power that is away from the citizen and into the hands of unaccountable and potentially untrustworthy third parties who may be bureaucrats or private sector companies.

Fourth, civil society has at times been more active in publicly discussing data sharing activities than the respective governments involved. If this paper cites civil society and academic research more than government documents, white papers, and research reports it is not by virtue of any particular bias, it merely reflects availability of materials. The United Kingdom (U.K.) is much more inclined to do consultations on these issues, and make research public, to cite merely one example. Some excellent materials have also been produced by other data protection authorities with the understanding that such documents and tools must be read in the context of relevant law, authorities, and the particular information initiatives in their jurisdictions. Scholarly attention to data sharing initiatives has come largely from the disciplines of political science and public administration and less so from privacy scholarship. Much of the theoretical work, while fascinating, offers little in the way of practical strategies for practitioners or the public.

Finally, the goal of this research is to provide a broad survey of the topic, potential frameworks for analysis, and a critical examination of some of the actions taken to protect privacy. If this report triggers a broader discussion of data sharing then this is even better.

II. Silos and Their Discontents

Around 2000, the rallying cry "let's break down the silos" started to be heard. The goal was to make greater use of information stored in its own sealed column – or silo – within an agency, isolated from the rest of the government and the rest of the world. In Canada, this coincided with attempts to do "joined-up government" or to cut administrative costs by amalgamating services. Reviewing some of the history allows us to see how the practices and issues developed.

In Canada and abroad, public administration went through a series of fundamental paradigm shifts, as governments at the federal, provincial, and municipal levels responded to change. While resource constraints are a constant, the recession of the early 1990s and the pressure to reduce massive deficits constrained government services. Rapid growth of the population and complexity brought on by changing patterns of movement and immigration became more evident in the 1980s and 1990s. The 20th century, with its two world wars, resulted in considerable immigration and population movement in Canada, but before the 1960s there were far fewer government support services, such as pensions, universal health insurance, and unemployment insurance. The constant march of technology paints an important backdrop to the fiscal, population, and administrative developments.

---

[4] For an analysis of why OECD countries experienced slow uptake of e-government services, see OECD, *Rethinking e-Government Services: User-Centred Approaches* (2009), http://www.oecd.org/gov/public-innovation/rethinkinge-governmentservicesuser-centredapproaches.htm. This is discussed in the examination of e-services.

The advent of computing power basically came in three waves, with large single purpose mainframes in the 1960s and 1970s, desktop computing in the 1980s, and networked computing in the 1990s. Public administrations responded by introducing government reform or "administrative renewal". Former TBS Secretary Ian Clark led an initiative for administrative renewal that led up to "Public Service 2000". The initiatives for "joined-up government" were in full stride by 2001 when the Auditor General analyzed them.[5] It is interesting to note the scarcity of references to the impact of the onset of desktop computing, email, and electronic services in the Auditor General's report. One can easily forget that no one had actually done business this way before. In the 1980s, IBM Selectric typewriters were on the desks of administrative assistants, and word processing pools typed documents from longhand drafts.

Given the lack of attention to what was a fundamental labour shift and learning challenge, it is not surprising that public servants at all levels often lacked the insight necessary to determine what was fair information practice with respect to the personal information of clients. The next wave is now big data and risk profiling, and it is hard to find government white papers discussing this reality either. The discourse is rather thin, so there are few shared understandings of what is ethical and respectful of human rights as "big data" is embraced.

It is often forgotten today that the U.S. was a world leader in privacy starting in the 1960s. A quick history of activities in the U.S. illustrates how the growth of privacy awareness and battles over dismantling data silos have been inextricably intertwined.

Early attention to privacy in the U.S. followed proposals to link disparate data systems. A 1965 study proposed creation of a National Data Center with authority to obtain computer tapes and other machine-readable data produced by all federal agencies. Opposition was strong enough that committees in both Houses of Congress began privacy hearings. A similar proposal, this time called FEDNET, emerged in the early 1970s. Vice-President (later President) Gerald Ford and the Congress stepped in to stop the idea.[6] More congressional privacy hearings followed.

In 1973, a federal advisory committee issued a highly influential report titled *Records, Computers and the Rights of Citizens*.[7] The report is most noteworthy for its proposal of Fair Information Practices (FIPs) as core principles for protecting privacy of personal information.[8] The committee recommended a privacy law for federal agencies, and Congress enacted the committee's ideas as the *Privacy Act of 1974*.[9]

One of the committee's five FIPs sought to limit uses and disclosures. The committee's precise statement of the policy was, "There must be a way for an individual to prevent information about him obtained for one purpose from being used or made available for other purposes without his consent."

---

[5] Auditor General of Canada, Public Service Management Reform: Progress, Setbacks and Challenges (2001), http://www.oag-bvg.gc.ca/internet/english/meth_gde_e_10222.html.
[6] Robert Ellis Smith, Ben Franklin's Web Site: Privacy and Curiosity from Plymouth Rock to the Internet 309-313 (2004).
[7] *Records, Computers and the Rights of Citizens*, Report of the Secretary's Advisory Committee on Automated Personal Data Systems (U.S. Department of Health, Education & Welfare, 1973), http://epic.org/privacy/hew1973report/default.html.
[8] For more background on Fair Information Practices, see Robert Gellman, *FAIR INFORMATION PRACTICES: A Basic History* (2014), http://ssrn.com/abstract=2415020.
[9] Public Law 93-579, 5 U.S.C. § 552a, http://www.law.cornell.edu/uscode/text/5/552a.

The objective of limiting the use of personal information to the original purpose is in many ways at the heart of the struggle over data silos. When can data collected for one program be used for another program? Who decides what the purpose of collection is? When and how are changes in programs, law, and purposes recognized and implemented? Do general government activities (e.g., audits, law enforcement, statistical activities, and archives) fit in with the purposes for any given program? Is the purpose test too unrealistic in a complex governmental environment? Where does individual consent fit in to determining how information can be used and disclosed? Is it realistic to rely on individual consent?

The objective of limiting the use of personal information to the original purpose is in many ways at the heart of the struggle over data silos.

In enacting the *Privacy Act of 1974*, Congress confronted these questions. The law sought to set standards for nearly all government record keeping systems containing personal information. What legal standard would govern use and disclosure limits for so many disparate government programs? In this report, the focus is only on disclosure.

Drafters of the law recognized that they could not define the purposes for all government data systems in a general statute. The law expressly allowed disclosures for auditing and other general government activities.[10] Because tying disclosures strictly to a purpose standard was seen as impractical, the law gave agencies considerable discretion on a program-by-program basis. The particular instrument was something called a "routine use".[11] A routine use is a disclosure that is "compatible with the purpose for which the record was collected."[12] Agencies define routine uses for each system of records through a rule making process that includes public comment.

We need not pause long to consider the vagueness of the compatibility standard or the reliance on it around the world.[13] The U.S. *Privacy Act of 1974* does not define the term "compatible", nor does it define "purpose". The result gave agencies the ability to provide for disclosures without the need for further legislative approval, without express reference to a clear legal standard, and without regard for consumer expectations.

In Canada, a similar problem was experienced with the federal *Privacy Act.* The law permitted the use of information within an agency for a "use consistent" with the purpose of the collection, and soon the number of consistent uses – or as it came to be interpreted, consistent purposes – mushroomed.

---

[10] PIPEDA has a clearer statement tying disclosures to the original purpose together with an entire principle devoted to identifying purposes. It also has exceptions broadly similar to those in the Privacy Act of 1974. See § 7(5).

[11] The term is confusing because a routine use is in common current usage an external disclosure rather than an internal use.

[12] 5 U.S.C. § 552a(a)(7), http://www.law.cornell.edu/uscode/text/5/552a.

[13] Compatibility is not just an American response to the problem of limiting disclosures. Compatibility plays a role in the EU Data Protection Directive. Article 6 provides in part that Member States shall provide that personal data must be: (a) processed fairly and lawfully; (b) collected for specified, explicit and legitimate purposes and not further processed in a way *incompatible* with those purposes. http://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:31995L0046&from=en.

During the early 1990s in Canada, the federal Committee for Administrative Renewal in Services looked at the forces that prevented information sharing, expecting to find the 1982 *Privacy Act* as the deterrent. In fact, the barriers came from other legislation and regulation that explicitly enjoined departments to not disclose information and to maintain confidentiality. Human self-interest during a period of major government downsizing brought on by the recession and double digit interest rates reinforced the legal barriers. IT departments and service delivery groups were anxious to hang on to their own turf and their own data. Thus, when the rallying cry to "tear down the silos" began echoing in federal circles and in the federal/provincial discussions on e-services, it should have been clear that privacy legislation was not the only or even the principal barrier.

It was hoped that in the leap to e-services, development of common platforms would eliminate some of the technical barriers to data sharing and common services. Mainframe systems, programmed in COBOL, and with fixed data input capability and fields, are difficult to merge. New and more flexible platforms can more readily accommodate data requirements of various departments and agencies. However, several factors combine to make sharing difficult to achieve in Canada, particularly as compared to other parliamentary democracies like the U.K.

- Services to citizens are inherently split between federal and provincial levels, with pensions, income tax, unemployment and disability benefits administered federally; and education, health, motor vehicle permits, and welfare administered provincially, sometimes municipally. Policing is even more complicated. Quebec administers income tax, the Canada Pension Plan, and immigration under its special arrangements. Compared to the U.K., where these services are all centrally managed and funded, it is easy to see why the U.K. has moved so rapidly for centralized systems, and why Canada has found it challenging. Privacy analyses rarely discuss the division of federal and state powers, but federalism is definitely a determining factor in data relationships.[14]
- Transborder dataflow to the U.S. is both a reality and a bogeyman. Virtually all Canadian Internet traffic is ported through the U.S., all under-sea cables terminate in the U.S. not in Canada, and satellite traffic is carried to a significant extent on U.S. satellites. Cloud services are typically U.S.-based and controlled. This is not well understood by the populace as a whole. When discussion of personal data being held in the U.S. arises, there is often an overreaction that belies the facts.[15] Having said that, when data is not in Canada, it is harder to enforce Canadian law, notably privacy law.
- The opening up of trade in government procurement means that any big systems are accessible to bidders from foreign states. The possibility that even more Canadian data

[14] Ian Clark discusses this in his paper "Distant Reflections on Federal Public Service Reform in the 1990s" included in the Auditor General's report cited above, see http://www.oag-bvg.gc.ca/internet/english/meth_gde_e_10222.html. Ross Anderson also discusses the threats of centralized databases in the report commissioned by the Rowntree Trust, *Database State,* http://www.jrrt.org.uk/publications/database-state-full-report.

[15] In Canada, questions about PIPEDA were asked concerning why there were not stronger provisions against cross-border dataflow in the legislation. The European Commission was particularly interested when determining adequacy. However, it is not well understood by the population as a whole, just how integrated our communications infrastructure was at that time, and it is arguably more so now. Transborder dataflow has been the driver for many discussions of privacy, certainly at the OECD and the Council of Europe, but also between the European Union and the rest of the world.

might be processed by companies from other countries could raise outsourcing concerns similar to those that drew a sharp policy reaction in the recent past.[16]

It should be noted that history is repeating itself with the availability and implementation of cloud services. In theory, cloud services eliminate the need to actually own servers and systems, allowing instead that departments lease space in the "cloud" and use shared software. This is not substantively different, from a privacy perspective, from leasing space on giant mainframes. Having access to everyone else's data that happens to be on the same cloud, however, is a different story.

Benefits of Breaking Down the Silos

The benefits of data sharing do not solely accrue to the governments or organizations that collect, use and disclose the information. There are definitely benefits to the citizenry. While this paper does not dwell on the reasons for data sharing/amalgamation, it is necessary to understand the reasons why it can be desirable. Anyone who has ever changed provinces with children in school and elderly parents in need of healthcare or residency in long-term care would fight hard for one-stop shopping, and single source address change. Some of the following benefits exist today, but not many because the merger of systems and coordination of services has proven difficult to manage. The potential benefits include:

Anyone who has ever changed provinces with children in school and elderly parents in need of healthcare or residency in long-term care would fight hard for one-stop shopping, and single source address change.

- Convenience for the citizen: Not being asked for the same data many times, potential one stop shopping (e.g., address changes);
- Better program delivery through a comprehensive or clustered approach: Why not have an automatic transfer of driver's license when changing provinces, simply by filing the new address? Why not get new license plate stickers in the mail? The essence of citizen-centred service is not profiling, it is trying to help citizens in certain groups or clusters get all the services they are likely to use or need;
- Automatic entitlement to programs for faster response: A good example of this is the Canada Pension Plan and Old Age Security pension. Why does Service Canada not simply enroll everyone since they know everyone's birthdate, and can get them into the system automatically when they turn 65? This program, being rolled out in 2013-14, has been difficult to engineer on aging mainframe systems. Parents applying for a social insurance number at birth, at the same time as they name their child and register the birth, has not only been one of Service Canada's more popular new programs, but it has improved the accuracy of the social insurance number database.
- Better risk management and cost control: Everyone benefits from reining in fraud. Duplicative services also cost money in administration, staff, and systems. However, it

[16] The outsourcing of health data processing in B.C. springs to mind, see British Columbia. Office of the Information and Privacy Commissioner. *Privacy and the USA Patriot Act: Implications for British Columbia Public Sector Outsourcing*. 2004. https://www.oipc.bc.ca/special-reports/1271. There are numerous other examples but few as well-documented.

cannot be assumed that savings will always result. Ross Anderson et. al point out in *Database State* that government IT projects do not always save money. In fact, the authors claim that whereas in the private sector roughly 35% of projects fail, in the public sector 70% fail[17];

- Efficiency: Effective use of data (i.e., accountancy, see Auditor General's report[18]), and the potential for new data mining techniques to create knowledge;
- Better information dissemination and training: One of the benefits of a holistic approach to government modernization and innovation is the ability to communicate information to citizens effectively about more than one program. Disparate projects require communications targeted to that individual program, and the citizen has only so much bandwidth to spend on figuring out how to do things and get service. The Centrelink case study in chapter six is a good example of an attempt to achieve this holistic approach. This also applies to communicating the rules to staff who need to know how programs inter-relate in order to give good advice to clients, and to follow the rules and legislative requirements themselves. The training value of effective client communications for staff should not be underestimated. Transparency for the citizen is also transparency for government employees at all levels, and in all areas of administration. A good program that provides concise, complete information about services can be useful to staff who have to administer other or parallel programs. Training and information distribution are problems that have not necessarily been solved in the information age; in fact, most public servants complain about information overload.

Risks of Data Centralization, Distributed Shared Access, and Data Mining

Fears of giant databases have been around since the 1960s, and in Canada were examined exhaustively by the federal departments of justice and communications, in *Privacy and Computers*[19]. Now the fears include data mining activities, not necessarily confined to a database or data warehouse, because data mining can more easily take place across platforms. Specific risks or worries include:

- Use of data for purposes unrelated to the purpose for which the data was collected;
- Loss of control of data by agencies;
- Inability to correct errors as data travels;
- Outdated/incomplete records (e.g., criminal history records without dispositions);
- Conflicting time periods resulting in incorrect linkages and inferences;
- Decisions made using unrelated, inaccurate data without the knowledge of the citizen;

---

[17] http://www.jrrt.org.uk/sites/jrrt.org.uk/files/documents/database-state.pdf, at pp 4, 44.

[18] Auditor General of Canada, *Report of the Auditor General of Canada to the House of Commons, Managing Identity Information* (2009), http://www.oag-bvg.gc.ca/internet/docs/oth_200902_e_32154.pdf. This report stemmed from a parallel audit conducted by the Auditor General and the federal Privacy Commissioner of the same four departments looking at the effective use of identity information. There is a great deal of useful commentary on Canada's failure to come up with a comprehensive and effective strategy for e-government services and the use of identity information, which backs up our later observations of the Lac Carling process.

[19] *Privacy and computers : a report of a Task Force established jointly by Department of Communications/Department of Justice,* Ottawa: Information Canada, 1972.

- Hostile users (i.e., the citizen may not know which organization ultimately holds and uses the data, and there may be no trust relationship);
- Profiling and the possibility of discrimination (e.g., potential Charter issues);
- Lack of accountability, either through imprecision among agencies with respect to mandate and applicable law, because of imprecision as data is managed/shared with the private sector or because no agency has clear authority to address and resolve errors;
- Absence of enforceable rights (e.g., due process);
- Legal complexity and difficulty in protecting rights because of sharing among federal/provincial/territorial agencies, including First Nations and across borders;
- The consequences of greater transparency. Generic disclosures might not accomplish true transparency, but if individuals were to get a ping on their phone every time an organization looked at their credit file, processed something in their bank, or checked their communications, people would suffer interminable interruptions;
- Knowledge gap of citizens is perhaps the most important risk of them all. People fundamentally do not understand how powerful data mining techniques are, how much data analysis exists today and has been going on for decades, or who uses their personal data;[20] and
- Feelings of utter powerlessness when individuals realize how much the technology can do, how far the data can travel, and how risks they never imagined could compromise their well-being.

These risks point to a glaring need for more informed public discourse on the topic of data sharing and data analytics. Statistically reliable data mining requires large stores of data, hence the desire for giant data warehouses. Prolonged or cumulative public sector data mining may tend towards the "snowball" technique of information gathering. This is a standard technique in ethnographic research where the researcher gleans an interesting piece of information from an interview or observation, and then follows it to gather more related information. For instance, a large number of border crossings of an individual who has been on unemployment insurance, gathered through the E311 cards described in one of the case studies in chapter five, through a port in Canada near a site of illegal activity (e.g., trafficking of duty-free cigarettes) might cause surveillance to focus on the individual and create a cluster of new information gathering. Expanded surveillance is one of the consequences of "know your customer" legislation[21], of which there are several instances in Canada, most notably in the financial and transportation sectors. For data mining purposes, there may be little data that is not theoretically worth sifting, and this flies in the face of current data protection law focused on purpose limitation, data collection limitation, and consent.

---

[20] Peter Schaar, former data commissioner for Germany recently published a call to arms on data mining in a special edition of MIND http://www.collaboratory.de/images/1/11/PrivacyandInternetGovernanceMIND7.pdf. Responses to how to preserve privacy and individual rights in the age of big data will certainly be the challenge of the next decade.

[21] Elsewhere this report notes the criticism of the previous federal Privacy Commissioner on her audits of the Financial Transactions and Reports Analysis Centre of Canada (FINTRAC) https://www.priv.gc.ca/media/nr-c/2013/nr-c_131024_e.asp. It is unlikely that most citizens are aware of what happens to their financial transaction data.

Data Mining and Big Data

Many terms appear in the popular and IT press about the topic of data mining, including big data, risk profiling, data analytics, predictive analytics, regression analysis, knowledge discovery, and so on. The reality of affordable data analytics software lurks behind almost all recent discussion of data sharing. It is beyond the scope of this paper to go into a detailed discussion of current data analytics capability, but it is important to understand what a data sharing initiative might envision in 2014 and beyond. There is also a need to be acutely aware that these tools are what IT firms sell today and have been marketing for the past 15 years. Governments have become convinced of the worth of these products and services. Cloud services, data warehouses, and data analytics software are hallmarks of modern IT systems. Noting all of the IT system failures in governments around the world in recent years, it is difficult to know if all are necessary or even useful, but vendors market them effectively and IT managers want the latest tools, not just to do the job but to maintain their own marketability.

We also need to be acutely aware that these tools are what IT firms sell today and have been marketing for the past 15 years. Governments have become convinced of the worth of these products and services.

In May 2014, the White House tabled a report entitled *Big Data: Seizing Opportunities, Preserving Values*[22] after a 90-day review and call for comments. Their definition of big data is as follows:

> Most definitions reflect the growing technological ability to capture, aggregate, and process an ever greater volume, velocity, and variety of data. More precisely, big datasets are "large, diverse, complex, longitudinal, and/or distributed datasets generated from instruments, sensors, Internet transactions, email, video, click streams, and/or all other digital sources available today and in the future."[23]

This appears to be a broad definition that fails to provide a test that readily distinguishes so-called big data from other data.

The White House report discusses the promises of big data:

- Big data can save lives through outbreak of disease detection.
- Big data can make the economy work better through sensors on jet engines and trucks, which can monitor hundreds of data points and send automatic alerts about the need for maintenance.
- Big data can save taxpayer dollars by using predictive analytics to detect fraud in healthcare providers.

---

[22] http://www.whitehouse.gov/the-press-office/2014/05/01/fact-sheet-big-data-and-privacy-working-group-review.
[23] Executive Office of the President, 2014. *Big Data: Seizing Opportunities, Preserving Values.* Accessed September 22, 2014 from http://www.whitehouse.gov/sites/default/files/docs/big_data_privacy_report_5.1.14_final_print.pdf.
The quote cites National Science Foundation, Solicitation 12-499: Core Techniques and Technologies for Advancing Big Data Science & Engineering (BIGDATA), 2012 http://www.nsf.gov/pubs/2012/nsf12499/nsf12499.pdf.

Risks were identified:

- Big data can alter the power balance between the citizen and the state.
- Big data, particularly "data fusion" or putting together multiple sets of de-identified data can re-identify the individual and result in invasion of privacy.
- Big data can lead to discrimination and profiling.[24]

The authors observe that many of the benefits attributed to big data appear to be unrelated to the use of identifiable personal information and many remain unproved.

The authors of the White House report offered six policy recommendations:

- **Advance the [Obama Administration's] Consumer Privacy Bill of Rights** because consumers deserve clear, understandable, reasonable standards for how their personal information is used in the big data era.

- **Pass National Data Breach Legislation** that provides for a single national data breach standard, along the lines of the Administration's 2011 Cybersecurity legislative proposal.

- **Extend Privacy Protections to non-U.S. Persons** because privacy is a worldwide value that should be reflected in how the federal government handles personally identifiable information from non-U.S. citizens.

- **Ensure Data Collected on Students in School** is used for Educational Purposes to drive better learning outcomes while protecting students against their data being shared or used inappropriately.

- **Expand Technical Expertise to Stop Discrimination** because the federal government should build the technical expertise to be able to identify practices and outcomes facilitated by big data analytics that have a discriminatory impact on protected classes.

- **Amend the Electronic Communications Privacy Act** to ensure the standard of protection for online, digital content is consistent with that afforded in the physical world—including by removing archaic distinctions between emails left unread or over a certain age[25].

These are modest recommendations that may have significant value, although most have little or nothing to do with so-called big data activities. It is not clear that, in the unlikely event that all the recommendations were implemented, they would meet the challenge of mitigating the risks identified. These include the creation of a power imbalance that threatens democracy, complete personal data collections on individuals gleaned from widely disparate sources, discrimination from invisible profiling that goes unnoticed because of the dynamic nature of data analytics, and unaccountable bureaucracies. Unfortunately, many of the touted benefits of big data that includes personal information are, to a privacy advocate, a worst nightmare. "Perfect personalization" is not just a risk from the discrimination perspective. Many see it as a fundamental invasion of privacy.

---

[24] Summarized in the *Factsheet*: http://www.whitehouse.gov/the-press-office/2014/05/01/fact-sheet-big-data-and-privacy-working-group-review

[25] Factsheet, http://www.whitehouse.gov/the-press-office/2014/05/01/fact-sheet-big-data-and-privacy-working-group-review.

The World Economic Forum launched a multi-year project entitled "Rethinking Personal Data" in 2010. The Forum published a series of reports and surveys[26] on personal information and data mining, proclaiming this explosive new personal information economy as "the new oil". Much of the discourse is aimed at transforming the attitudes to sharing personal information, persuading consumers that there is value to themselves in permitting their devices to surveil their movements and choices, and in developing options for data protection law that replaces concepts of the fundamental right to be left alone.

The authors note that, despite the above, there is healthy skepticism elsewhere in the privacy world about whether privacy needs to make accommodations to so-called big data. The International Working Group on Data Protection in Telecommunications published a report on big data in May 2014[27] which takes an entirely different view of the matter. They have enumerated a number of risks and recommendations, which provide useful guidance. The introduction to this paper notes the recent skeptical comments of the Article 29 Working Group[28], and the authors expect that it is likely there will be further focus on the matter by data protection commissioners, as cases and complaints reach them.

This paper cannot resolve here the new issues raised by data mining or by so-called big data. These more current issues are discussed because the pressures of new buzzwords and new analytics are not dissimilar from the pressures of old analytics and the allure of vast promises made by those who would break down silos without regard to the consequences or even the likelihood of success. What follows is more backward looking, seeking to draw lessons from the past and to suggest how those lessons can be applied to the data sharing challenges of the future.

III. A Short International Overview

This short chapter, while heavily influenced by Canadian law, reviews some considerations in international data protection law and practice that should be kept in mind when looking at the examples in the following chapter.

For data sharing conducted by governments in the delivery of services to individuals, the constitutional framework in which an organization operates is as important as the relevant data protection law. Data protection law tends to broadly permit government organizations to gather personal information when authorized by law. Whether any actual practice is too intrusive must often be settled in court with reference to the constitutional protections of that jurisdiction. This can be a slow process. One of the more difficult positions in defending privacy or data protection law is arguing that the practice in question is illegal. These cases do not progress through the courts at the

---

[26] Personal Data: the Emergence of a New Asset Class (2011); Rethinking Personal Data, a New Lens for Strengthening Trust (2014); The Internet Trust Bubble Global Values, Beliefs and Practices (2013).
[27] *Working Paper on Big Data and Privacy: Privacy principles under pressure in the age of Big Data analytics*, http://www.datenschutz-berlin.de/content/europa-international/international-working-group-on-data-protection-in-telecommunications-iwgdpt/working-papers-and-common-positions-adopted-by-the-working-group.
[28] http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp221_en.pdf.

speed that IT progresses, and that is a fundamental problem. This paper includes an analysis of recent court decisions that relate to data sharing in the following chapter. However, first it is important to look at a few underlying issues in data protection law.

European law focuses on the concepts of "proportionality" and "necessity". Whether data collection or sharing benefits are proportional so as to outweigh intrusions to the privacy of the individuals concerned is relevant. The Article 29 Data Protection Working Party published a recent opinion[29] on the relevance of the concepts of proportionality and necessity in the context of law enforcement activities. This discussion is informative with respect to data sharing.

The working party notes that the concepts evolved from and must be understood in light of the European Convention on Human Rights (ECHR), notably Article 8(2). The working party cites recent jurisprudence in which the European Court of Human Rights (ECtHR) set out three criteria to be examined in considering whether an interference with an individual's rights under Article 8(2) is justified. An interference with an individual's Article 8 rights must be:

- in accordance with the law;
- in pursuit of one of the legitimate aims set out in Art. 8(2); and
- necessary in a democratic society.

The European Union's (EU) Data Protection Directive (DPD), which has had such a profound influence on privacy law, passed before the European Commission had competence in law enforcement matters. It therefore was silent on matters of police and intelligence. Convention 108 of the Council of Europe did cover these matters, but one of the reasons that the DPD was developed in 1990 was that few member states actually had data protection law reflecting the requirements of Convention 108. Canada had a similar situation at the time with few provincial laws reflecting Canada's commitment to adhere to the Organization for Economic Co-operation and Development (OECD) Guidelines on the Protection of Privacy and Transborder Flows of Personal Data.

Canadian data protection law does not use the word "proportionality" nor do the OECD Guidelines on which Canadian laws are loosely based. Instead, Canadian law focuses on "purpose", on "consent", and on "limiting collection" to that which is necessary. In public sector laws, generally consent is not a requirement; rather, legislative authority for collection is required.

At first glance, this may not provide much clarity with respect to whether a data sharing initiative is acceptable from a privacy perspective.

Legislation crafted to provide authority to run a program, such as healthcare, education, or employment insurance, may not have extensive sections dealing with the matter of personal information. Consent for data collection may be meaningless in the context of administering programs, such as education and healthcare. Attention in these programs has focused on the ability to opt out of certain disclosures as well as on the ability to restrict data flows to only those who need

[29] Opinion 01/2014 on the application of necessity and proportionality concepts and data protection within the law enforcement sector, http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp211_en.pdf.

to know. The extent to which privacy is considered in the design and drafting of government programs and their enabling legislation is obviously variable. Where laws say little about privacy, it may be unclear what, if any, privacy standards were applied in making judgments that reflect the balancing of interests implied by proportionality concerns. These issues were given extensive scrutiny by the U.K. Law Commission, in their consultation on data sharing[30], and they have arisen in the discussions in Europe during the development of the new General Data Protection Regulation[31].

It is apparent from some of the case studies reviewed in this paper that sorting out what is acceptable under existing Canadian data protection law is not always easy. There appears to be ample room for policy development.

IV. Constitutional Backgrounder

Privacy, the Charter, and Information Sharing

The *Canadian Charter of Rights and Freedoms* (Charter) protects the fundamental rights and freedoms of persons against state action. This is set out in section 32, which reads:

> 32. (1) This Charter applies
>
> a) to the Parliament and government of Canada in respect of all matters within the authority of Parliament including all matters relating to the Yukon Territory and Northwest Territories; and
>
> b) to the legislature and government of each province in respect of all matters within the authority of the legislature of each province. [32]

The Supreme Court of Canada (SCC) has interpreted this clause to mean that the Charter applies to all laws created by the executive, administrative, legislative[33] and judicial[34] branches of government.

Although the charter has been held to apply to rules and regulations created by government actors, it is not considered to extend to common law situations between individuals. Nevertheless, as legislation with a transformative as well as a remedial intent, the Charter is a normative document, setting out what is and is not acceptable practice in Canada generally, whether or not a given organization is subject to the Charter. This has meant that although relationships at common law are not subject to the Charter, the SCC has held that they should be interpreted in a manner consistent

---

[30] Law Commission Consultation Paper No. 214, *Data Sharing Between Public Bodies: A Consultation Paper (*2013). http://lawcommission.justice.gov.uk/docs/cp214_data-sharing.pdf
[31] http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52012DC0009&from=en
[32] *The Constitution Act, 1982*, Schedule B to the Canada Act 1982 (UK), 1982, c 11, http://canlii.ca/t/ldsx.
[33] *RWDSU v. Dolphin Delivery Ltd.*, [1986] 2 S.C.R. 573.
[34] R. v. Rahey [1987] 1 S.C.R. 588.

with the Charter.[35] This means that private sector organizations may, and should, review Charter standards in order to guide their own conduct.

The Charter does not contain the word "privacy" nor does it include a freestanding right to privacy. This does not mean, however, that there are no privacy interests implied in the Charter. Privacy interests have been recognized in various provisions of the Charter and are foundational to other protections granted by the Charter.

For this report, the two primary sections of the Charter that apply to privacy and information are sections 7 and 8.

Section 7 of the Charter states that, "[e]veryone has the right to life, liberty and security of the person and the right not to be deprived thereof except in accordance with the principles of fundamental justice."[36] The liberty interest in particular is grounded in privacy rights, especially in relation to an individual's control of their body and personal information. This has been articulated both in relation to a person's right to make choices that are at the core of individual dignity and independence[37] and an individual's right to informational self-determination.[38] It should be noted, however, that virtually all of the jurisprudence in this arena has been generated in the course of criminal and quasi-criminal proceedings; the extent, if any, of section 7 informational privacy rights outside that context it still a developing area and hence an uncertain one.

The other Charter section at issue, and more commonly invoked with regard to privacy, is section 8, which grants a right to be free from unreasonable search and seizure. Section 8 protects people and not places; in particular, it protects a biographical core of personal information which individuals in a free and democratic society would wish to maintain and control from dissemination to the state. This includes information which tends to reveal intimate details of the lifestyle and personal choices of the individual.[39] In order for a search to be reasonable, it must be (a) authorized by a law; (b) that itself is reasonable; and (c) the manner in which the search was carried out was reasonable.[40]

The SCC has decided that the source of the section 8 right is that citizens have a reasonable expectation of privacy in a free and democratic society. A reasonable expectation of privacy is to be determined on the basis of the totality of the circumstances. If an accused person establishes a reasonable expectation of privacy, the inquiry must then proceed to determine whether the search was conducted in a reasonable manner[41]

---

[35] Despite finding that the *Charter* did not apply to such situations, the Court did suggest that interpretation and application of the common law should be in accordance with the principles and values set out in the *Charter* even though the *Charter* didn't govern the situation. (*RWDSU v. Dolphin Delivery Ltd.*, [1986] 2 S.C.R. 573).
[36] Charter, s. 7.
[37] *Cheskes v. Ontario (Attorney General)*, 2007 CanLII 38387 (ON S.C.) paragraph 87, citing *R. v. Malmo-Levine,* 2003 SCC 74 (CanLII), [2003] 3 S.C.R. 571 at para. 85, quoting *Godbout v. Longueuil (Ville),* 1997 CanLII 335 (S.C.C.), [1997] 3 S.C.R. 844 at para. 66. Also see *Blencoe v. British Columbia (Human Rights Commission)*, 2000 SCC 44 (CanLII), [2000] 2 S.C.R. 307 at para. 83, at para. 49; *B.(R.) v. Children's Aid Society of Metropolitan Toronto*, 1995 CanLII 115 (S.C.C.), [1995] 1 S.C.R. 315 at 368-9; *R v. Morgentaler,* 1988 CanLII 90 (S.C.C.) , [1988] 1 S.C.R. 30.
[38] *R. v. O'Connor*, 1995 CanLII 51 (S.C.C.), at para. 120.
[39] *R. v. Plant*, [1993] 3 S.C.R. 281.
[40] *R. v. S.A.B.*, *2003 SCC 60*.
[41] *R. v. Edwards*, [1996] 1 S.C.R. 126; *Hunter v. Southam Inc.*, *[1984] 2 S.C.R. 145*.

Until recently, the jurisprudence around privacy seemed fully formed and unlikely to be subject to any major changes. *R v. Plant*, which dealt explicitly with the question of government access to (utility) records held on a computer, took direction from *R v Dyment's* citation of the Report of the Task Force on Privacy and Computers to the effect that:

> Consideration of such factors as the nature of the information itself, the nature of the relationship between the party releasing the information and the party claiming its confidentiality, the place where the information was obtained, the manner in which it was obtained and the seriousness of the crime being investigated allows* for a balancing of the societal interests in protecting individual dignity, integrity and autonomy with effective law enforcement. It is, then, necessary to apply this contextual approach to the facts of the case at bar.[42]

Applying these tests to the facts of that particular case, LaForest concluded that individuals held a reasonable expectation of privacy in a "biographical core of personal information which individuals in a free and democratic society would wish to maintain and control from dissemination to the state. This would include information which tends to reveal intimate details of the lifestyle and personal choices of the individual."

LaForest added that computerized records of electrical use did not meet this standard, and accordingly Plant was not considered to have had a reasonable expectation of privacy in that information such that section 8 rights were engaged.

Application of section 8 to informational privacy was further nuanced in *R v Tessling*[43] which reviewed the question of whether a reasonable expectation of privacy could be held with regard to heat emanations from an individual's home. In the course of their decision, the SCC spoke of privacy as a "protean concept" and separated the interests protected by section 8 into three categories: personal privacy, territorial privacy, and informational privacy. In contrast to Abella's (then a member of the Ontario Court of Appeal) decision that patterns of heat could reveal information about personal behaviour within the home, the SCC concluded that heat distribution information offered no insight into private life and further that its disclosure did not affect the dignity, integrity or autonomy of Mr. Tessling.

While these decisions bracket an approach to informational privacy that looks at the information at issue "objectively", denuded of context, this approach has been overruled in the June 2014 decision in *R v. Spencer*.[44] The case dealt with the question of whether subscriber information held by an Internet service provider was personal information from which there was a reasonable expectation of privacy. In making its decision, the SCC reiterated previous statements about the importance of assessing the totality of the circumstances, emphasizing that this lens "underlines the point that they are often interrelated, that they must be adapted to the circumstances of the particular case and that they must be looked at as a whole."[45] This early statement heralded a new, complex and ultimately more expansive understanding of the importance of informational privacy, one that reviewed

---

[42] *R. v. Plant*, [1993] 3 S.C.R. 281.
[43] *R. v. Tessling*, [2004] 3 S.C.R. 432.
[44] *R v. Spencer*, [2014] SCC 43.
[45] *R v. Spencer*, [2014] SCC 43.at para 17.

information not in isolation but rather incorporated an understanding of inferences and assumptions drawn from the information and their impact on privacy.[46]

Having broadened the information to be assessed in ascertaining the presence of a reasonable expectation of privacy, the SCC then proceeded to expand the nature of the privacy interest at issue. From the established understanding of informational privacy as primarily concerned with confidentiality and information control[47] the court moved instead to articulate three subcategories of privacy: privacy as secrecy, privacy as control, and privacy as anonymity.[48]

Discussing privacy as anonymity, the SCC writes:

> The notion of privacy as anonymity is not novel. It appears in a wide array of contexts ranging from anonymous surveys to the protection of police informant identities. A person responding to a survey readily agrees to provide what may well be highly personal information. A police informant provides information about the commission of a crime. The information itself is not private — it is communicated precisely so that it will be communicated to others. But the information is communicated on the basis that it will not be identified with the person providing it. Consider situations in which the police want to obtain the list of names that correspond to the identification numbers on individual survey results or the defence in a criminal case wants to obtain the identity of the informant who has provided information that has been disclosed to the defence. The privacy interest at stake in these examples is not simply the individual's name, but the link between the identified individual and the personal information provided anonymously.[49]

This expanded understanding of privacy to include an interest in anonymity is of particular importance when dealing with issues of data matching, data mining and other iterations of information manipulation that may result from breaking down the silos. This is made explicit by the SCC's continued discussion of the anonymity interest when it explains that:

> [m]oreover, the Internet has exponentially increased both the quality and quantity of information that is stored about Internet users. Browsing logs, for example, may provide detailed information about users' interests. Search engines may gather records of users' search terms. Advertisers may track their users across networks of websites, gathering an overview of their interests and concerns. "Cookies" may be used to track consumer habits and may provide information about the options selected within a website, which web pages were visited before and after the visit to the host website and any other personal information provided: see N. Gleicher, "Neither a Customer Nor a Subscriber Be: Regulating the Release of User Information on the World Wide Web" (2009), 118 Yale L.J. 1945, at pp. 194849; R. W. Hubbard, P. DeFreitas and S. Magotiaux, "The Internet — Expectations of Privacy in a New Context" (2002), 45 Crim. L.Q. 170, at pp. 189-91. The user cannot fully control or even necessarily be aware of who may observe a pattern of online activity, but by remaining anonymous — by guarding the link between the information and the identity of the person to whom it relates — the user can in large measure be assured that the activity remains private: see Slane and Austin, at pp. 500-3.[50]

---

[46] The recognition of the role of inference has already been recognized by *R. v. Kang-Brown*, 2008 SCC 18 and *R v. Gomboc* 2010 SCC 55.
[47] *R v. Spencer*, [2014] SCC 43.at para 34.
[48] *R v. Spencer*, [2014] SCC 43. at para 38
[49] *R v. Spencer*, [2014] SCC 43. at para 44 (emphasis added).
[50] *R v. Spencer*, [2014] SCC 43 at para 46

This recognition of a privacy interest that is engaged when various data are linked is a key one, and signals a new, informed and complex understanding of informational privacy that will surely impact any future Charter analysis that is applied to government information sharing, whether between government bodies or with private actors. This is an extremely important development, and signals the importance of developing a new discourse on data sharing and in particular data analytics.

A final note with regard to this expanded understanding of informational privacy interests: as discussed, organizations often seek to justify information sharing by pointing to the importance of protecting the public whether from criminal interests or for security purposes. In that context, it should be noted that *R v Spencer* deals with a situation that involved child pornography – an important and emotional public and criminal issue. Despite this, the SCC is clear as to where and how the analysis must be performed, emphasizing that the analysis must focus on the question of how the search impacts on the privacy of its target rather than on whether that privacy is protecting nefarious, criminal or otherwise problematic behaviour, "[T]he issue is not whether Mr. Spencer had a legitimate privacy interest in concealing his use of the Internet for the purpose of accessing child pornography, but whether people generally have a privacy interest in subscriber information with respect to computers which they use in their home for private purpose."[51]

Any analysis of information sharing must, therefore, take as its starting point not the interests that the government seeks to advance, but rather the impact upon privacy of the proposed information sharing. Obviously privacy alone will not be determinative, and even where the privacy interest is violated it may be saved by section 1 of the Charter, which guarantees the rights and freedoms set out in it subject only to such reasonable limits prescribed by law as can be demonstrably justified in a free and democratic society.[52]

Right to Be Forgotten

There has been considerable discussion, mostly in Europe, about the right to be forgotten. This relates to the fact that if anything has ever been on the Internet, it is likely still there if one searches either long enough or cleverly enough. This flies in the face of data retention schedules, and since data is being mined from the Internet for profiling it is relevant to this research.

Furthermore, given the appetite for data that has more longevity in order to detect patterns better, there is a risk of having the concept of data deletion abandoned within government record systems. In this respect, it is important to note the case of the Financial Transactions and Reports Analysis Centre of Canada (FINTRAC), which requested the ability to retain data for an additional three years in order to improve pattern analysis. The amendments were passed in 2006.[53] Since FINTRAC's reason for existence is to track patterns of money transfer in order to find money laundering and terrorist financing, these amendments seem reasonable. FINTRAC agreed to regular audits by the Privacy Commissioner to balance this intrusion, which seems commendable risk mitigation. However, a press release from the Privacy Commissioner of Canada indicates, the first audit in 2009 found FINTRAC was retaining too much data, as did the audit in 2013[54]. When a

---

[51] *R v. Spencer*, [2014] SCC 43, para 36.
[52] *R v. Spencer*, [2014] SCC 43 at s. 1.
[53] https://www.priv.gc.ca/media/nr-c/2009/nr-c_091117_e.asp
[54] https://www.priv.gc.ca/information/pub/ar-vr/ar-vr_fintrac_2013_e.pdf

covered institution over-reports, as organizations are inclined to do because there are criminal penalties for failing to report, FINTRAC has no means to filter these reports out so retains them. This is a good example of the difficulties of today's data environment where the cost of collection and retention have shrunk to nothing, whereas the work in filtering out bad, irrelevant or outdated information could be significant, and requires human intervention and expense.

An important European case, however, relates to the Internet and to Internet search engines. In May 2014, the European Court of Justice (ECJ) issued its decision in the Google Spain "right to be forgotten" case[55].

The case was initiated in 2010 when a Spanish citizen found that the results of a Google search of his name included a 1998 newspaper article detailing his debt status and the forced sale of his property. Given that it was 10 years later and he had resolved the financial issues, he felt that the link should not still be available. After both the newspaper itself and Google refused to remove the information, he complained to the Spanish data protection authority (AEPD). After investigation, the AEPD ordered Google to remove the links, but Google challenged the ruling eventually leading the case to the ECJ.

The decision is in stark contrast to the preliminary ruling in June 2013 where the ECJ's Advocate General did not agree that Google was a data controller and thus had no obligation to delete the links. The full court found that, in fact, the operator of a search engine does collect, retrieve, record, organize, disclose and store information and accordingly does fall into the category of data controller. As a data controller, Google was found in this case to have an obligation to remove the data. However, the obligation to remove data was not put forward as always applicable or absolute with the court instead recognizing that there were certain situations in which such removal would be appropriate; and that the individual's rights of informational self-determination must be balanced against the interests of the public in knowing or having access to the information.

Identifying the catch-22 implicit in the decision, Harvard Law School Professor Jonathan Zittrain commented on his blog that:

> In fact, I can't tell if the Spanish citizen actually won anything. The Court's own press release names him, and the fact that he at one point owed so much money that he had a property foreclosed. Not only does that illustrate the Streisand Effect, giving attention to exactly the thing he wanted to keep private, but more important, it appears to show that the Court doesn't see a problem with publishing the very data it thinks sensitive enough to be worthy of an entirely new category of protection.[56]

The decision garnered much media coverage and expert comment forecasting everything from business as usual to the end of the Internet as we know it. Perhaps the most balanced (and honest) response came from the Information Commissioner's Office in the U.K., which essentially congratulated the court for including Google under the rubric of EU data protection law and

---

[55] *C-131-12* http://curia.europa.eu/juris/document/document_print.jsf?doclang=EN&text&pageIndex=0&part=1&mode=DOC&docid=152065&occ=first&dir&cid=437838 for the European Commission's factsheet on the case, see http://ec.europa.eu/justice/data-protection/files/factsheets/factsheet_data_protection_en.pdf

[56] http://blogs.law.harvard.edu/futureoftheinternet/2014/05/13/is-the-eu-compelling-google-to-become-about-me/

promised discussion on the practical implications of the decision once there had been an opportunity to review and consider the decision.

In a May 2014 article, ABC News spoke about the right to remove "unflattering" information, and characterized the process as censorship used by persons to polish their reputations.[57] Putting it in these terms, however, is oversimplified and dismissive. The decision does not provide carte blanche for anyone to request the removal of any information for any reason. In fact, the Google form is clear that in order to make a request, the following information is required:

a) Provide the URL for each link appearing in a Google search for your name that you request to be removed.
b) Explain, if it is not clear, why the linked page is about you
c) Explain how the URL in search results is irrelevant, outdated or otherwise inappropriate

Even after this information is provided, there is no guarantee that the removal request will be approved. Google says[58] that in addition to the reason provided by the user, requests will be assessed to determine whether there is a public interest in the information, such as information about financial scams, professional malpractice, criminal convictions, or public conduct of government officials. Although other search engines that function in the EU have not yet announced[59] their own processes for complying with the decision, some similar considerations can be expected to be factored in.

It is indisputable that reputation has increasing importance, and that the availability of a wide swathe of information via search engines is an integral part of reviewing that reputation and of making risk and trust assessments based upon it. That said, reputation is most effective when the information that is available is reliable and relevant. The point should not be to keep any and all information available but rather to ensure the accuracy of the information that is available. To conflate informational self-determination with censorship is problematic enough, but to use such a characterization in order to defeat the basic precepts of data protection[60], which include accuracy and limiting information to what is necessary, is more than problematic – it is destructive both of individual rights and the potential power of reputation.

As indicated at the beginning of this section, the right to be forgotten is an important concept for this research. It shows how a basic requirement of data protection as designed during the 1970s – the right to have outdated and unnecessary personal information deleted when it was no longer accurate or relevant – has become controversial when applied in the context of the Internet. Previously, old data in most systems was unlikely to be used. Currently, there is a far greater likelihood that it will be used for data analysis or potentially found by the curious. Just as data matching became commonplace and rules against it ignored when search capability grew with modern data platforms, data retention and destruction schedules have become neglected as data storage costs have plummeted. It is now more difficult to delete data than to keep it, but that does not mean the function is any less necessary for the protection of privacy.

---

[57] http://abcnews.go.com/Technology/wireStory/google-taking-requests-censor-results-europe-23922152
[58] http://online.wsj.com/article/SB10001424052702303633604579593151552354742.html
[59] http://www.euronews.com/2014/05/31/google-offers-right-to-be-forgotten-form-to-remove-personal-data/
[60] http://ec.europa.eu/commission_2010-2014/reding/multimedia/news/2014/05/20140531_en.htm

V. Case Studies and Analysis

Using the basic principles of analysis outlined in the introduction, this chapter examines data sharing activities in 12 examples, in seven different jurisdictions. The examples were chosen using the following criteria, noting that some examples made it onto the list for only one or two of the criteria:

- Is there good information available about the activity?
- Does this case demonstrate an important point or case in law?
- Was the issue resolved?
- If the data sharing ceased, was there an important lesson?
- Are there best practices to be captured?
- Is there ongoing study or activity in this case?
- In the case of older examples, are there interesting parallels in today's IT environment?

The examples include simple data matching, e-government initiatives (which may or may not always involve data sharing), joined-up government, and data mining.

1. Australia: The Australia Card

- **WHO:** Australian Taxation Office, the former Department of Social Security, the former Health Insurance Commission, and the former Department of Immigration and Ethnic Affairs

- **WHAT:** Universal and compulsory identification card containing name, photograph, signature, identification number, and expiry date

- **WHERE:** Australia

- **WHY:** To create a population register and a reliable identification document

- **WHEN:** Introduced in 1986, withdrawn in 1988; revisited in 2006 as the health and social services access card, withdrawn in 2007

- **HOW:** Smart card with magnetic strip repeating data on the card; and creation of a national register which multiple agencies could access

The attempts of several Australian governments to introduce identity cards are of direct interest to data sharing because government issued identity cards can be a precursor to the sharing of personal information by government agencies through central registers or otherwise. The Australian proposals are famous in the lore of national identity cards. The Australia Card had actually already gone into production in 1987 when it was withdrawn based on a public uproar. The introduction of

the card was also the trigger for the creation of one of the more resilient and long-lasting global NGOs working on privacy issues, namely the Australia Privacy Foundation (www.privacy.au.org).[61]

The Australia Card was launched in 1987, with a proposed Act of Parliament that was never supported by the Senate, but technically could still have been passed by the ruling government. The features of the system included:

- A register containing name at birth or on arrival, current name, nicknames, aliases, date of birth and death, sex, citizenship status, residential and postal addresses for the past two years, and Australia Card number.
- De facto mandating: the card was necessary to obtain services such as receipt of pay with appropriate tax, operation of bank accounts, social security or health benefits, even though acquiring a card was not technically mandated by law.
- No prohibition of other unauthorized uses and no effective controls on secondary use (i.e., a nightclub could insist on production of the card and copy the information).
- Enforcing organizations, such as a hospital or bank, were required to see the card at time of transactions and record the number.
- Enforcing organizations were required to forward new information, such as a change of address, to the register.
- Children's cards contained a date of birth, prompting suspicion that the plan was a reliable proof of age record.
- Computerized storage of the photo and signature, which were groundbreaking features in 1987.
- The register recorded all accesses to the database by accredited agencies, thus creating an auditable transaction record.
- Other agencies, while not having access to the register, were required to provide information to it, including the departments of defense, veterans' affairs, education, and foreign affairs and trade, and the Australian Electoral Commission. While this sounds Orwellian, the stated purpose of doing so was to update address and death information.

Opposition to the card came from all sides – right, centre, and left. There were severe fines for employers who hired someone without a card, or for farmers who tried to deal with marketing boards without a card. The business applications of the card created broad opposition among groups who might otherwise have been expected to endorse government efficiency. Even rock stars and sports heroes protested. One notable dissenter was Ben Lexcen, who had just won the America's Cup in yachting, the first time that a non-U.S. team had won. He went on national television saying he would burn his citizenship before he accepted the card. Australians marched in the streets, and divisions started to arise in caucus ranks as letters of protest flooded officials and newspapers. The government discovered a flaw in the legislative scheme and withdrew it in October 1987.

In 2006, the Department of Human Services tried again with a proposed "health and social services access card". This card had a chip, and the following features:

---

[61] This account relies extensively on the work of the founders of the Australia Privacy Foundation, notably Graham Greenleaf's article in the *Law Society Journal* (NSW) Vol. 25 No. 9, October 1987, and his later article in the *Computer Law and Security Report* 23(2007) comparing the two cards ("Australia's proposed ID card: Still quacking like a duck"), and on material published by Roger Clarke and Simon Davies on the APF website.

- The government assured the public that it was not and would not become a national identification card;
- The card was not compulsory, but it was the only form of identification acceptable for Medicare or other government benefits;
- A registry similar to the one proposed in 1987; and
- Much more capacity for storage of "voluntary data".

The proposal for the access card was withdrawn by the Labor government after the election in November 2007. This is an example of a data sharing proposal being abandoned as a result of a change in political leadership. Note that the card was separate from the Centrelink project (see next case study) as a whole, although it would have performed a function for that project.

Conclusions

- Within various western governments, this saga is well known, even though it is reaching the stage of being ancient history. The Australia Card is cited as an example of what happens when the public gets excited about something that seemed to be a sensible plan to bureaucrats.
- Whether a good idea or not, the Australia Card was not developed with adequate participation by all stakeholders. The government failed to lay a proper policy foundation with the public for its proposal. Proponents failed to take privacy and other objections into account as they developed and tried to roll out the card.
- The card affected too many constituencies at once which generated widespread opposition.
- High profile data sharing activities that directly affect individual citizens often receive more attention than data sharing that occurs quietly between government departments out of the direct sight of data subjects, but which may have equally significant privacy concerns.
- NGOs and privacy activists can organize quickly and have a huge impact on government projects given the right circumstances and leadership. They tend to have long memories. Dr. Roger Clarke still carries his tattered Australia Card in his wallet.
- Privacy was a relatively new issue when the card was first proposed in 1987, but the card failed anyway.

2. Australia: Centrelink Master Program

- **WHO:** Department of Human Services
- **WHAT:** New government organization set up to manage shared services
- **WHERE:** Australia
- **WHY:** Duplication of services
- **WHEN:** 1997 - ongoing
- **HOW:** Separate operating agency with common platforms for data

The Australian government knew of service duplication, especially when it came to the welfare and employment insurance departments. Previous government attempts to address this duplication by contracting out case management had not achieved the desired results. As the full extent of duplication became evident – not just services but clients and policies as well – the idea for Centrelink was born.

Centrelink was originally set up under legislation in 1997[62] with the mandate to:

> s.8A: (a) to provide services, benefits, programs or facilities that are provided for by the Commonwealth for a purpose for which the Parliament has the power to make laws; (b) to provide services, benefits, programs or facilities that are provided for a person other than the Commonwealth, for a purpose for which the Parliament has the power to make laws.

Centrelink included any services, benefits, programs or facilities where the chief executive of Centrelink or departmental employees are involved in:

- making payments in connection with the services, benefits, programs or facilities;
- making decisions in connection with the services, benefits, programs or facilities;
- collecting information in connection with the services, benefits, programs or facilities; or
- providing information about the services, benefits, programs or facilities.

While the services included were extensive, Centrelink did not include Medicare programs, or services, benefits, programs or facilities provided under the *Child Support (Assessment) Act 1989* or the *Child Support (Registration and Collection) Act 1988*. The Minister has the power to exclude services by regulation.

Despite undertaking to provide nominally public services, Centrelink was established as a government organization but with a quasi-private sector organizational model. A Memorandum of Understanding created a series of business partnership agreements (BPA) between individual departments and Centrelink. The agreements set up the funding structure for Centrelink, wherein the departments pay Centrelink for services. Each BPA set out details of the services, the funding arrangements, agreed performance outcomes, allied reporting mechanisms, and outlined arrangements for the sharing of information and for dealing with unforeseen issues.

A board of management was responsible for the administration and oversight of Centrelink, including establishing the overall objective for the organization, providing strategic direction and setting out business rules and policies. The Minister for Family and Community Services appointed the board. The board also reported to the Minister on any administrative issues within the Minister's portfolio. Secretaries of the individual client departments were members of the board. The Australian National Audit Office provided additional oversight. Despite the private sector organizational model, Centrelink remains a public sector body and is subject to the Auditor General's investigation and reporting functions.

After 2000, Centrelink increased the programs for which it provided service and broadened the scope of those programs. These changes were part of a move from a service-based model towards an

---

[62] http://www.austlii.edu.au/au/legis/cth/consol_act/hsa1997266/.

individual-focused model where life events became the organizing principle. As part of this move in 2002, a new "customer account" system was rolled out. This system displayed customer information in a single view. Ultimately this system was intended to be easily accessible to the individual allowing people to maintain and update their information.

The 2008 Gershon Report[63] – an independent review of the Australian Government's use of information and communication technology (ICT) processes intended to maximize the benefits of ICT while also striving for greater efficiency and improved services – recommended a move towards whole-of-government ICT service provision. Building on this, the Minister for Human Services introduced the idea of service delivery reform (SDR) in 2009. This reform called for human services agencies to be co-located in order to facilitate enhanced service delivery and cost-savings, and to guard against fraud. There was some suggestion that another motivation for the centralization of human services might be to lay the foundation for some kind of identity card.[64]

As the SDR moved forward, concerns arose about what integration might mean. Privacy advocates, among others, worried that centralizing services might also mean combining and sharing information, data processing, software and other ICT resources.[65] The department clarified that the intent was not to create one central database and that the distinct customer databases held by each individual agency would remain separate; however, there would be a shared service platform created for common use rather than combining all information.

The department emphasized that any data sharing would be based on a consent model where customers have the option to consent in advance to sharing of their information or of not opting into the information sharing meaning that they would have to provide information anew for each program and agency. Finally, the department pledged to work with the Australian Privacy Commissioner's office to ensure that privacy safeguards are built into the system.[66]

In 2011, under the *Human Services Legislation Amendment Act 2011*[67] SDR became a reality, with Medicare Australia, Centrelink, and CRS Australia[68] all being integrated into the Department of Human Services. This meant, among other indicia of cooperation, the creation of a single telephone number and website through which clients could access different services.

As of January 2011, clients register for an account at www.australia.gov.au. Account holders can access their Department of Human Services account using a single identification and password. As of June 2011, 42,000 users signed up for an account.

The SDR document[69] indicates that part of the reform process is the integration of frontline services delivery, corporate functions, and ICT infrastructure platforms and systems.

---

[63] P. Gershon (2008). *Review of the Australian Government's Use of Information and Communication Technology*. http://www.finance.gov.au/publications/ICT-Review/
[64] http://www.rogerclarke.com/DV/SDR-0912.html.
[65] http://www.itnews.com.au/News/213723,centrelinks-data-centre-plans-spark-privacy-concerns.aspx.
[66] http://www.itnews.com.au/News/213723,centrelinks-data-centre-plans-spark-privacy-concerns.aspx.
[67] http://www.comlaw.gov.au/Details/C2011A00032.
[68] Australia's disability support and assessment agency, formerly known as Commonwealth Rehabilitation Services.
[69] http://www.humanservices.gov.au/spw/corporate/about-us/resources/service-delivery-reform-overview.pdf.

The current *Bilateral Head Agreement 2012-2015*[70] contains a section addressing information and information management, including sharing of information between agencies and access to databases "as appropriate". Compliance and program integrity – terms that describe fraud detection and enforcement – are also mutually supported. In today's world of big data, compliance and program integrity may involve data analytics for risk assessment.

Conclusions

- The Centrelink project appears to be a success. It succeeded where the Australia Card failed in part because Centrelink provided specific services to individuals whereas the Australia Card was more disembodied from any overt benefit to individuals.
- Centrelink provided individuals with some degree of control and choice, allowing those with specific privacy concerns to tailor their experience with Centrelink. This may have quieted those who might otherwise have been most vocal about privacy.
- In proposing smart cards, Centrelink "established consultative arrangements with privacy advocates, and with consumer interest representatives of clients of Centrelink and its client agencies".[71] That description of consultation comes from a leading Australian privacy consultant and advocate, not from Centrelink. Consultations with issue advocates and representatives of those affected by data sharing programs are likely to produce better outcomes and increased acceptance.
- Over time, Centrelink built up a large number of users. Providing service and convenience can prompt citizens to ignore privacy issues, as has been seen with any number of private sector services. This does not mean that privacy is a dead issue, but it may reflect the way risk analysis is calibrated by the average individual.
- It is noteworthy that the *Bilateral Head Agreement 2012-2015* has no explicit mention of privacy or data protection, but buries it in the expressions "where appropriate" and "within the legislative framework". From a privacy perspective, the agreement is not overly transparent.
- In-depth analysis of the private sector partners that participate in government information sharing initiatives is beyond the scope of this report, but the authors note that in most jurisdictions, the IT business sector actively promotes solutions (e.g., data warehouses, analytics software, single sign-on authentication standards, risk management, use of outside customer data bases) and sometimes plays a key role in establishing partnerships and data platforms.[72] In many jurisdictions, consultant studies develop approaches to government data sharing because as Anderson et al. point out, IT expertise and training in government has not been able to keep up with the challenges.[73]

---

[70] http://www.humanservices.gov.au/spw/corporate/about-us/resources/bilateral-head-agreement.pdf . The agreement is between the Department of Human Services and the Department of Health and Ageing.
[71] Roger Clarke, Centrelink Smart Card Technical Issues Starter Kit (1998), http://www.rogerclarke.com/DV/SCTISK.html.
[72] See the platform described in the UK children' services projects for a toolkit approach to municipal data sharing, http://www.fame-uk.org.
[73] Anderson et al, Database State p.46.

3. Canada Provincial: British Columbia Services Card

- **WHO:** Ministry of Health, Insurance Corporation of British Columbia (ICBC), and Ministry of Technology, Innovations and Citizens' Services
- **WHAT:** Development of shared identity management system and smartcard credential
- **WHERE:** British Columbia
- **WHY:** Enhanced and efficient service delivery, fraud reduction,
- **WHEN:** February 2013 – ongoing
- **HOW:** Smart card (contactless) which in final phase 2018 will communicate with databases within British Columbia (B.C.) as an identity credential; photo templates for facial recognition programs and databases remain separate

In 2011, the B.C. Government established a multi-year, multi-phase project intended to develop a smartcard credential and associated identity information management system; implement the cards and put them into the hands of users; and then build a system where access to various government services is available using the cards and identity information services.

The project had multiple stakeholders, including the Ministry of Health, ICBC, and the Ministry of Technology, Innovations and Citizens' Services.[74] Together they created a card that combines two of the most used services, which already require a card – drivers' licences and health cards. This partnership was created in order to leverage the respective strengths and mandates of each organization. The Ministry of Health administers the Medical Services Plan (MSP) in which 99 percent of B.C. residents are enrolled. MSP has the most comprehensive client base of all public sector programs.

In order to issue drivers' licences and manage car and driver insurance, ICBC provides province-wide infrastructure, technology, and best practices for in-person identity proofing and card issuance. The Ministry of Technology, Innovations and Citizens' Services has the mandate to improve service delivery for citizens. The program was enabled by legislative amendments to the *Freedom of Information and Protection of Privacy Act* (FIPPA) in November 2011 that established the legal authority for collection and disclosure of personal information by the designated Provincial Identity Information Services Provider (PIISP). In addition, amendments to the *Motor Vehicle Act* (MVA) and the *Medicare Protection Act* (MPA) authorized ICBC and the Ministry of Health to partner with the Ministry of Technology, Innovation and Citizens' Services to develop and implement the BC Services Card.[75] Beginning in February 2013, the government introduced the new BC Services Card,

[74] http://www.cio.gov.bc.ca/cio/idim/bcservicescard.page.
[75] https://www.oipc.bc.ca/news-releases/1502.

which replaced the B.C. CareCard.[76] All individuals between the ages of 19 and 74 must obtain a BC Services Card before February 2018. The card must be renewed every five years.

The BC Services Card is government-issued identification that allows its holders to provide authentication of their identities and access provincial services. At present, this means health services and drivers' licenses. The stated intent of creating the central card is to enhance service provision, improve patient safety, reduce card misuse, and provide future in-person and online access to other government services. The card will provide a central point of access to more services in the future.

There are two different versions of the card – a combined B.C. driver's license and BC Services Card, or a BC Services Card only, which may or may not contain a photograph. The cards will contain the following information:

- first and last name;
- card issuance date;
- card expiry date;
- date of birth; and
- indication whether the card may or may not be used as a driver's licence.

The cards also contain a variety of identifiers and technological mechanisms, including:

- personal health identification number;
- magnetic strip, used for scanning and reading card data;
- barcode; and
- chip.

Both the magnetic strip and barcode contain the same information that appears on the card. The chip does not store personal or medical information.[77] The B.C. Government site assures users that their personal information is kept secure through security measures on the card (i.e., photograph, magnetic strip, anti-forgery design, and chip). Privacy remains protected because the individual silos of information will not be aggregated. For example, healthcare providers have access only to health information while a law enforcement officer or ICBC employee can view driver's licence information but not health information.[78]

Concerns

Upon the announcement of the program, various groups raised privacy concerns. The Information and Privacy Commissioner of B.C. reviewed phase one – the enrolment of individuals and issuance of the card – and while the Commissioner had determined that that this phase met all legal requirements, there were recommendations made for the ongoing implementation of the program:

---

[76] Five year project with budget of $150 million, http://www.cbc.ca/news/canada/british-columbia/powerful-new-card-to-replace-b-c-care-card-1.1354302.
[77] http://www2.gov.bc.ca/gov/topic.page?id=C71B580C55204AAC98B35C6B75D8860D&title=Photo%20BC%20Services%20Card.
[78] http://www2.gov.bc.ca/gov/topic.page?id=1AEB073331D547448009E506D6DAC395

- the development of a retention policy for access and audit logs, and a destruction schedule;
- that the transfer of personal information be protected by payload encryption, and that 256-bit encryption be employed to protect personal information in transit; and
- that as the program expands, new parties and clients to the BC Services Card should be required to demonstrate the adequacy of their privacy management programs to the Ministry of Technology, Innovations and Citizens' Services before entering into this initiative.

In addition, the Commissioner expressed disappointment that no public consultation had been undertaken at the outset of the project and suggested that a full consultation take place prior to phase two. The Commissioner indicated an intention to continue to monitor the program, including reviewing:

- employee training manuals developed for the BC Services Card initiative to better understand how internal attacks may be mitigated and managed;
- changes, if any, to the Integrated Program Agreement between the three partners;
- new privacy impact assessments (PIAs) and information sharing agreements as subsequent phases of the program evolve and new public bodies join to use the platform;
- government's tool to assess the readiness for programs and agencies that wish to access BC Services Card in future phases;
- notice of any new collection of personal information in this phase; and
- the program's disaster recovery planning to determine what policies and procedures are in place to mitigate a dedicated denial of service type of attack, and what transpires in the event identity authentication services are unable to be provided.

The Commissioner was not the only voice raising concerns about the program. The B.C. Civil Liberties Association (BCCLA) and the B.C. Freedom of Information and Privacy Association (FIPA) publicly supported the Commissioner's call for a public consultation. These groups also suggested that the consultation be expanded into an inquiry into the government's track record of privacy-invasive, security-weak and costly IT projects generally, asking for the consultation prior to implementation of the BC Services Card initiative.[79]

Drs. Kate Milberry and Christopher Parsons, supported by the B.C. Civil Liberties Association and the Office of the Privacy Commissioner of Canada's research contributions program, also released an extensive report entitled *A National ID Card By Stealth? The BC Services Card: Privacy Risks, Opportunities and Alternatives*.[80] The report critiques the privacy implications created by the data linkage as well as the security vulnerabilities created by the scope of the project.[81] At every step, the report interrogates the program within its full context by looking at it not only as proposed but placing it within a larger move towards national federated identity management. Their review of the program and its technological underpinnings concludes that "[p]otential weaknesses in the BC Services Card arise around card issuance and forgery, data management and security processes, the

[79] http://bccla.org/news/2013/02/privacy-groups-demand-halt-to-bc-id-card-roll-out/.
[80] http://www.christopher-parsons.com/Main/wp-content/uploads/2013/11/2013-National-ID-Card-by-Stealth.pdf.
[81] Id. at 10.

NFC chip, and function creep." They present a series of recommendations that address the technological issues and the policy implications:

- The public should be informed (in plain language) of the proposed identity system, including the on-going costs and business case for the proposal. An evidence-based business case should be presented to support any and all justifications for the program.
- Stakeholder consultations followed by a publicly available report of the results of the consultations.
- Federal and provincial Information and Privacy Commissioners should work together to fully review the idea of a federated identity system.
- In order to guard against function creep, the B.C. Government should clearly define potential future uses and services that may be associated with the BC Services Card over the next years.
- Best practices would also support the government setting out a checklist of what conditions should be met prior to linking a new service to the BC Services Card infrastructure
- Development of overarching security standards and a focus on user-centric privacy protective models that incorporate technological protections.
- Given that the card(s) rely on biometrics, care must be taken to ensure that the potentially invasive nature of the biometrics is proportional to the benefits.

The government proceeded with a consultation[82] in late 2013, with the intent of understanding B.C. citizen values and determining how to build public trust in the process. The consultation consisted of an online public survey that elicited more than 1,100 responses[83]; a focused two-day expert panel consisting of more than 100 experts in identity management, privacy and related fields; and a BC Services Card User Panel consisting of 35 randomly selected citizens representing a diverse range of ages and backgrounds who then gathered in Vancouver for a series of workshops.

At the end of the process, the user panel identified a number of services that they felt could benefit from association with the BC Services Card identity authentication model. Among the services identified were:

- online access to health records, lab results, prescription history and renewals;
- student loan applications;
- birth, death and marriage certificate applications;
- disability bus pass applications; and
- general confirmation of a citizens' eligibility for services.[84]

As for the consultation itself, in April 2014 the government released a report that contained not only the results of the consultations but the government's responses[85] to those recommendations. While broad commitments about openness, transparency and the protection of privacy resulted, little specificity appears to have resulted from the consultation.

---

[82] http://www.bcbsides.ca/bc-services-card-consultation/.
[83] http://www.gov.bc.ca/citz/down/DigitalServicesConsultation_appendix3.pdf.
[84] http://www.gov.bc.ca/citz/down/DigitalServicesConsultation_appendix2.pdf.
[85] http://www.gov.bc.ca/citz/down/DigitalServicesConsultation_report_web.pdf.

Conclusions

- It is too early to offer firm conclusions about the impact of public and privacy concerns on the BC Services Card, but relevant points of view are now being heard in the decision-making process.
- Whether or not the government initially undertook adequate consultations with the public, it appears that efforts at public consultations expanded over time in response to criticism.
- The Information and Privacy Commissioner of B.C. had an opportunity to review the project at various phases of the project and provided useful advice.
- The Millbery/Parsons report demonstrated the importance of funding for civil society and academia to complete research on current issues. This report usefully informed discussion of the issues.
- The government apparently paid attention to the interventions of the B.C. Information and Privacy Commissioner. In any case, there is far more transparency about this initiative than there has been in the case of federal initiatives, which is examined next.

4. Canada and the Provinces: Single Sign-On and E-Services

It is outside the scope of this report to provide a complete history of the federal/provincial/territorial (FPT) official discussions on shared services. What follows is a brief snapshot of how we got to where we are today. The Lac Carling meetings discussed below are really a process, and not yet a data sharing project.

- **WHO:** FPT officials involved in electronic services, including chief information officers (CIO) and management board officials. Federal officials involved in electronic services, led by Treasury Board of Canada Secretariat (TBS), Shared Services Canada (SSC), Service Canada, and assisted by Public Safety Canada (PSC), and Communications Security Establishment Canada (CSEC) experts.

- **WHAT:** Regular meetings and committee work to develop common platforms for identity management, single sign-on, and, where possible, joint-service delivery options

- **WHERE:** Canada

- **WHY:** Since the mid-1990s, it was recognized that if all 14 FPT jurisdictions developed separate methods of identifying citizens for e-government services money would be wasted and security risks unmitigated. TBS played a lead role in organizing the first sessions, called the Lac Carling meetings, named after the location of the first conference.

- **WHEN:** 1995 - ongoing

- **HOW:** The initiative encompasses a wide-range of information sharing activities, joint ventures, and threat-risk analysis. Records of the meetings and publications generated by the conference shed light on Canada's version of joined-up government.

The Lac Carling meetings were started in 1996 by the TBS, bringing together officials from all jurisdictions, as well as private sector IT companies, in an effort to kick-start the desired

transformation of government e-services.[86] Coordinated e-services and identity management has been slow to coalesce although different jurisdictions over the years have introduced their own e-services. The federal initiative, Modernizing Services for Canadians, had a three-year plan for 2003-05, which saw the establishment of Service Canada, and the development of one-stop service centres. The magazine *IT World Canada* covered the Lac Carling meetings over the years, and it wrote in 2006 that the 10th annual Lac Carling meeting appeared to be a turning point as municipalities initiated practical trials and projects for e-services.[87] One sample project that *IT World* identified as an example of how inter-jurisdictional projects could work was web platform BizPal that several municipalities tested:

> BizPaL (www.bizpal.ca) is a permit and licence identification system. Integrated into municipal Web sites or portals, it gives business owners and entrepreneurs a single point of contact so they can find out what permits and licences their businesses will need from municipal, provincial/territorial and federal governments.[88]

It is interesting that this is a business example (i.e. does not involve personal information) and is basically what is referred to as an "information-out" application, namely one where general information is dispensed to users through an interface but no data is stored from the user. It does, however, sort municipal, provincial and federal licence requirements in a way that takes advantage of web service capability. Efforts to coordinate on identity management have been painfully slower.

TBS released a strategy, *Federating Identity Management in the Government of Canada: A Backgrounder* in 2009, and that appears to be the latest document[89]. The public sector CIO council continues to work on these projects.

SSC proposed architecture for authenticating government employees, called ICAM[90], but there appears to be no public summary or evaluation of the success of that project. No authentication scheme has been rolled out to citizens as yet. Authenticating individual citizens is a harder problem than government employees who have lower expectations of privacy in their workplace context than citizens. As described in the BC Services Card case study, B.C. appears to have led on this particular initiative authenticating citizens for a range of services. It remains to be seen whether other provinces or the federal government will follow B.C.'s lead.

Given that the Lac Carling discussions have gone on for so long, and are really the forum for FPT discussions of joined-up government (as will be described in the U.K. case study), it is interesting that progress on joint efforts appears to be slow. There is little official material publicly available so it is difficult to evaluate developments. Canada has not been studied in the OECD study series on e-

---

[86] It is worth noting by way of background here, that during the 1990s, the federal Department of Justice and the Treasury Board Secretariat worked with UNCITRAL (United Nations Commission on International Trade Law) to determine the technical and legal parameters to shift government documents and contracts from paper to electronic format. The last half of PIPEDA is the legislation drafted to put into effect our commitments at UNCITRAL, and PIPEDA was the enabler of e-commerce in some respects. Treasury Board promoted this work as well, at the Lac Carling meetings.
[87] http://www.itworldcanada.com/article/lac-carling-x-a-turning-point/633#ixzz3BL4ppBgK
[88] http://www.itworldcanada.com/article/lac-carling-x-a-turning-point/633#ixzz3BL4ppBgK
[89] http://www.tbs-sct.gc.ca/sim-gsi/docs/2011/fimgc-fgigc/fimgc-fgigc01-eng.asp
[90] http://itac.ca/wp-content/uploads/2013/07/AFAC_Cloud-Computing_-Challenges-_July-2013.pdf.

government although it is interesting that a Canadian chairs the committee[91], and the CIO of TBS chairs the e-leaders committee.

IT Canada has reported on most of the meetings, but the departments concerned have not. The CIO of TBS has given many speeches about the events of Lac Carling, yet there is no website for the group. Municipalities appear more organized, having established their own association, meetings and website.[92] The action by municipalities seems to correspond to the experience in the U.K. It is interesting to compare the experience of Canada and the U.K. to that of Denmark (as will be described in case study 12).

Conclusions

- It is difficult to comment on why Lac Carling has gone on for so long with so little public transparency except to say that it is in sharp contrast to the progress in other countries as indicated by the OECD series of country reports on e-government.[93]
- The initiative started with a focus on authenticating the individual for centralized service and data sharing. The fact that this forum appears to have become less active in the area of identification authentication may indicate the difficulty of the task.
- Privacy has never been a key focus of this conference, although the topic was recognized as a potential barrier to data sharing and a working group was developed to study the issue.
- Civil society does not appear to have participated in the development of the recent OECD guidance on e-government, and it would be useful if civil society were more active in these matters.

5. Canada: E311 Data Matching

- **WHO:** Department of National Revenue (Customs), Canada Employment Insurance Commission (CEIC) and Department of Human Resources and Skills Development Canada (HRSDC)

- **WHAT:** Sharing of E311 information between CRA and HRSDC

- **WHERE:** Canada

- **WHY:** Employment insurance (EI) eligibility investigation and enforcement

---

[91] Joe Wild, undersecretary of Cabinet at the PCO, chaired the public governance committee, while Corinne Charette chaired the OECD Network on E-government, which released in July 2014 guidance on Digital Government Strategies http://www.oecd.org/gov/public-innovation/recommendation-on-digital-government-strategies.htm. It is noteworthy that the guidance recommends that governments take a risk-based approach to privacy. It would perhaps have been preferable to take a human rights based approach supplemented with comprehensive risk assessment.

[92] http://www.misa-asim.ca/.

[93] https://www.oecd.org/governance/observatory-public-sector-innovation/countryprofiles/canada/ Note that Canada has chosen to submit its documents on streamlining the Public Service (*Blueprint 2020: A Vision for Streamlining Canada's Public Service* http://www.clerk.gc.ca/eng/feature.asp?pageId=361) but no work on E-government, as compared to Denmark, case study number 12 in this paper.

- **WHEN:** 1995 - ongoing

- **HOW:** Data matching between the records of two agencies facilitated by data processing via Statistics Canada (StatsCan).

This case study is described in some detail because the data sharing was contested and went to the SCC. The program is an illustration of a classic data match and the difficulties inherent in such a match. The E311 cards are handwritten by travellers, but only the cards filled out by individuals crossing the border by air or train were scanned and stored on microfilm. HRSDC, now known as Employment and Social Development Canada, later hired the federal department, StatsCan, to convert the data into a machine-readable format that could be matched with the EI files.

Department of National Revenue (Customs)

Under section 11(1) of the *Customs Act*, persons arriving in Canada must present themselves to an officer of the Department of National Revenue (Customs), now known as Canada Border Services Agency, when they arrive at a Canadian port of entry at which time they must answer any questions asked by the officer in the performance of duties under the *Customs Act* or any other Act of parliament. The questioning typically relates to the regulation of importation of goods, including the application of taxes, fees, etc.

Where the entrance to Canada is by air, persons arriving must also complete the E311 Customs Declaration Card and provide the information requested on that form – name, address, date of birth, flight number, carrier's name, point of origin, date of departure from Canada, date of return, value of products purchased, amount of personal exemption claimed and place of arrival. This information includes personal information about the traveler and their families.

Employment Insurance

The *Employment Insurance Act* sets up a worker compensation scheme to provide economic and social security for a period of time in case of loss of income through loss of employment. HRSDC or its operational arm, Service Canada, administers EI.

EI relies on self-reporting by claimants. When filing a claim for benefits under the *Employment Insurance Act*, claimants receive information about their rights and obligations while receiving benefits. These include the obligation to search for and be available for work at all times. Among other things, this means that claimants are not entitled to receive benefits under the *Employment Insurance Act* for any period during which they are not in Canada unless the absence falls within an exception prescribed by the *Employment Insurance Regulations*. Within those parameters, claimants are expected to regularly provide information establishing their entitlement to benefits.

Data Sharing

Following a request by the CEIC[94], Customs agreed to disclose to the Commission information from the E311 cards. Customs' was of the opinion that since this information was to be used by the CEIC in the administration and enforcement of the *Employment Insurance Act*, the information could be released to the Commission under what was then section 108(1)(b) of the *Customs Act*, without offending the *Privacy Act*. In exchange, the CEIC agreed to use the information disclosed by Customs solely for the purposes of the *Employment Insurance Act* and not to disclose the information to any third parties. The CEIC already had wide powers to collect information for the purposes of the Act, but not specifically E311 card information.

The proposed sharing had four stages: a feasibility study including a cost-benefit analysis; a second feasibility study; a six-month pilot project; and full implementation planned at the end of 1997. The CEIC conducted a feasibility study on the merits of implementing the program in 1995. Following the study in January 1996, the CEIC notified the Office of the Privacy Commissioner of Canada of the program, proposing pilot matches for the period April 1, 1996 to October 1, 1996 and permanent implementation thereafter. This notification complied with the TBS policies on privacy and data protection.

Under the agreement between the parties, Customs made available to HRSDC certain information (e.g., traveler's name, date of birth, postal code, purpose of travel, and dates of departure and return to Canada) from E311 forms completed by Canadian residents returning to Canada by air. HRSDC, acting on behalf of the CEIC, then electronically matched the Customs data with the CEIC's database of EI claimants. After the data matching, the CEIC took further steps if needed to identify claimants who received benefits during unreported absences from Canada.

The Privacy Commissioner expressed concerns about the project, in particular:

- Lack of proportionality of the project, with the government conducting searches in the files of honest travelers and EI claimants in order to catch a few abusers;[95]
- Sharing of information beyond that necessary for the purpose[96];
- Lack of transparency and knowledge (i.e., travelers were not told that their E311 cards were going to be used for any purpose other than Customs)[97]; and

---

[94] The Employment Insurance Commission is the actual body with regulation making authority, not the Minister. See http://www.esdc.gc.ca/eng/jobs/ei/commission/.

[95] In the 1996/97 Annual Report, then Privacy Commissioner Bruce Phillips commented that "Doubtless such a match will catch some who may be cheating EI. But the price it exacts is far too high. It systematically searches millions of innocent travelers, without their knowledge or consent, who filed customs returns on the assumption - and on Revenue Canada's word - that they would be used for customs purposes only." See https://www.priv.gc.ca/information/ar/02_04_05_e.asp#014.

[96] "Only the name, address, date of birth and duration of the trip are relevant to the Department of Human Resources for matching purposes" Julien Delisle speech, 1998 http://www.priv.gc.ca/media/sp-d/archive/02_05_a_980128_e.asp.

[97] "The match offends the most fundamental principle of any privacy law; that government tell its citizens why it is collecting personal information, then use it only for that-and not a wholly unrelated-purpose (unless the individual consents). The reason for the principle is clear: to prevent the government from conducting unwarranted surveillance on its citizens by prowling through its immense personal databanks on what amounts to nothing more than high-tech fishing expeditions." Bruce Phillips, Annual Report of the Privacy Commissioner of Canada, 1996/97, https://www.priv.gc.ca/information/ar/02_04_05_e.asp#014.

- The absence of a written agreement setting out the conditions of the exchange.

After being assured that these issues would be resolved before the project's final implementation, the Privacy Commissioner informed the government that he would not oppose the pilot project. The program began operating in September 1996.

Implementation

In January 1997, the Privacy Commissioner wrote to the Minister of National Revenue and the Minister of Human Resources Development raising concerns about the program. In his letter, the Privacy Commissioner stated that he had obtained legal opinions to the effect that the program was unconstitutional. The expert consulted had concluded that the project was a breach of section 8 of the Charter and that the government had no solid grounds to justify the search of the files. According to the expert opinion, the data matching program had the same effect as giving law enforcement agencies full powers to search homes without first obtaining a search warrant duly signed by a judge.

During the implementation phase, Customs provided HRSDC, acting on behalf of the CEIC, with all the E311 cards stored since 1992. This raised additional concerns for the Privacy Commissioner, namely:

- As information used for an administrative purpose, the E311 cards should only have been retained for a period of two years;
- That Customs was able to provide forms dating back to 1992 indicated the retention of information beyond the period necessary; and
- The use of forms dating back to 1992 involved the retroactive application of the agreement.

In March 1997, the Minister of Human Resources Development wrote to the Privacy Commissioner and stated that, while claimants had already received ample direction to report their absences from Canada, additional steps were being taken to reinforce this obligation with them. In addition, to answer the concern over the retroactivity of the program, the Minister of Human Resources Development agreed that only cases dating back to January 1994 would be examined for possible overpayments and that there would be no prosecutions on any retroactive cases.

Critiques and Challenges

The Privacy Commissioner took the matter to the Federal Court, seeking a declaration that this disclosure of personal information was inappropriate. The government countered that the program was authorized by section 8 of the *Privacy Act* and section 108 of the *Customs Act.*

The court agreed that the travelers' information was personal information, under the control of Customs, and that section 8(2)(b) of the *Privacy Act* governed the disclosure. Personal information under the control of a government institution may only be disclosed for purposes that are in accordance with any Act of parliament or any regulation made thereunder that authorizes its disclosure. In this case, the appropriate Act was the *Customs Act* of which section108 (1)(b) allows disclosure of information to any person that the Minister may authorize subject to conditions that the Minister may specify.

The program in question was established pursuant to a blanket authorization, which allows the disclosure of information obtained for the purpose of the *Customs Act* when needed for the administration or enforcement of a law of Canada. It was the opinion of the court that the authorization issued by the Minister was an invalid exercise of his discretion. In previous cases[98], the court stated that the purpose of sections 107 and 108 of the *Customs Act* was to preserve the confidentiality of information gathered in the administration of the Act and to disclose it only in limited circumstances. In the case of this program, however, the court felt that the Minister's blanket authorization (i.e., purporting to authorize the communication of information for the administration or enforcement of, not simply the *Customs Act*, but of any Act of Canada or a province) exceeded the scope of the Act. Accordingly, section 108(1)(b) does not allow the Minister to authorize the investigation described in the memorandum of understanding because to do so would be an exercise of discretion contrary to the purposes of the *Customs Act*. The Federal Court, given this analysis, determined[99] that the data sharing was not authorized.

The Federal Court of Appeal reversed the decision[100] on the grounds that the Federal Court had erroneously focused on the 1991 blanket authorization when in fact it was the 1997 memorandum of understanding to which they should have turned their attention. When that analysis was done, the Federal Court of Appeal concluded that the information sharing was properly authorized under section 108(1) (b) of the *Customs Act*, in accordance with section 8 of the *Privacy Act*. The SCC, in 2001, issued a brief decision[101] dismissing the subsequent appeal and agreeing with the Federal Court of Appeal's decision.

A parallel court process was initiated in the name of Deborah Smith who was on vacation outside of Canada for two weeks in early 1995 while in receipt of EI benefits. Upon returning to Canada by air, she completed an E311 Customs Declaration Card. In January 1997, her E311 card was accessed under the data-match program and, as a result, the CEIC discovered that she had received benefits while out of the country and ordered repayment of those benefits. Ms. Smith raised Charter arguments, claiming both her section 8 protection against unreasonable search and seizure and her section 6 mobility rights were infringed by the data-sharing project. The Federal Court, Federal Court of Appeal[102] and SCC[103] all determined that there was no Charter violation. Despite the concerns of the Privacy Commissioner, this left both the program and the data sharing in place and officially endorsed as an appropriate sharing of information.

Since then, the information sharing has been codified in law and policy. The Canada Border Services Agency, successors to the Department of National Revenue (Customs), has a policy on the disclosure of customs information[104], most recently updated in September 2013. This document, among other things, breaks down the applicable sections of the Act, including section 107(5)(i) of the Act, which authorizes the provision of information to HRSDC, namely to "an official of the Department of Human Resources and Skills Development solely for the purpose of administering or

---

[98] *Glaxo Wellcome v M.N.R.* https://www.canlii.org/en/ca/fca/doc/1998/1998canlii9071/1998canlii9071.html.
[99] https://www.canlii.org/en/ca/fct/doc/1999/1999canlii9335/1999canlii9335.html.
[100] https://www.canlii.org/en/ca/fca/doc/2000/2000canlii17110/2000canlii17110.html.
[101] https://scc-csc.lexum.com/scc-csc/scc-csc/en/item/1931/index.do.
[102] https://www.canlii.org/en/ca/fca/doc/2000/2000canlii14930/2000canlii14930.html.
[103] https://scc-csc.lexum.com/scc-csc/scc-csc/en/item/1930/index.do.
[104] http://www.cbsa-asfc.gc.ca/agency-agence/reports-rapports/cd-da/pdci-pdrd-eng.html.

enforcing the *Employment Insurance Act*, if the information relates to the movement of people into and out of Canada".

This program and its results are a matter of no small importance. Court documents show that despite almost 29,000 claimants having properly reported their absence from Canada in 1995 and 1996 and accordingly having their EI benefits suspended for the period of their absences as a result, the program was still remunerative for the CEIC. As of November 1997, the program had resulted in disentitlements in 31,467 cases. As of August 1998, 98,914 disentitlements found overpayments in 83,749 cases totaling $55,146,255. In addition, 40,689 penalties had been assessed as of August 1998 as a result of the program.

Conclusions

- This is a good example of a case where an organization, wishing to do a data match, availed itself of the regulatory authority to do the match without getting additional Parliamentary authority, consulting with stakeholders, publicizing its plans, or any of the other processes expected in new and potentially invasive data sharing exercises. Given the relatively early date of the original proposal (i.e., early in terms of privacy), the lack of consultation may be understandable.
- While the lack of transparency about the match has been corrected, there were no repercussions for the initial lack of transparency.
- One can speculate that the actual savings reported from the data match may have had a bearing in the case. Wholesale perusal of the travel records of Canadians with no proof of benefits to the match might have been a more difficult case to argue. In U.S. data matching, savings or claims of savings from computer matching made it hard for privacy proponents to find political support. The Centrelink case study included in this paper demonstrates that service and convenience can trump privacy. This example suggests that cost savings can do the same.
- At one level, the Privacy Commissioner's decision to take the matter to court was not successful and resulted in a controversial program being found to be authorized. The specific result and the broader precedent were not good for privacy generally. The later legislative authorization placed some limits on the sharing of E311 card information, and that legislation may cut off different uses of the information without parliamentary approval. The choice of tactics makes a difference, and going to court is definitely playing for "higher stakes". However, win or lose, the case generated a great deal of necessary discourse on the issue of data matching, and may have accelerated the promulgation of other remedies, such as PIAs.

6. Global: The WHOIS Directory

- **WHO:** The Internet Corporation for Assigned Names and Numbers (ICANN) in cooperation with the Government Advisory Committee of ICANN, a committee of government representatives that imposes policy requirements on this non-profit corporation set up to manage the Internet domain name system (DNS)

- **WHAT:** A universal, globally accessible directory of the registrants of domain names known as WHOIS

- **WHERE:** Directory is globally accessible over the Internet, ICANN as a corporation is headquartered in California

- **WHY:** To create a DNS registry, and make information about owners of domain names available to all for the purposes of law enforcement, copyright and trademark enforcement, and consumer protection

- **WHEN:** The original system developed with the first Internet in the 1980s, but the formal WHOIS requirements were initiated in 1998 when ICANN was incorporated. Data collection and data retention and escrow requirements have grown over the years

- **HOW:** All registrars of domain names are required by contract to collect information from individuals and companies for generic top level domains (gTLDs) and make the data accessible through port 43 servers on the Internet

ICANN is one of the key players in international Internet governance. ICANN was established by the U.S. Commerce Department under a rough charter known as the Affirmation of Commitments[105]. ICANN is a non-profit organization incorporated in the state of California. It functions as a multi-stakeholder community, meeting in person three times a year, and meeting virtually to work on domain name governance issues through open working groups. The organization is remarkably transparent, but those who volunteer tend to have an economic stake in the results of policy and implementation discussions.

WHOIS, now mandated by ICANN through contracts with DNS registrars, is a query and response protocol widely used for querying databases that store the registered users of an Internet resource like a domain name. WHOIS had fairly innocuous beginnings rooted in the simple need for the early Internet developers to know who registered a given domain name in order to be able to address technical problems. This directory grew in parallel to commercial use of the Internet with its importance growing as domain names achieved greater importance. Trademark owners realized the risk to their brands if someone registered a domain name that violated or otherwise harmed their copyright or trademarks. Soon law enforcement also wanted access to information that would permit them to know who was the owner or registrant for a given website. The stakes grew quickly from technical to economic.

Along with the increase in those wanting access to WHOIS there was an expansion in the extent of information collected, going beyond the information necessary for technical stability (e.g., technical information about the Internet protocol addresses and root servers). New data gathering, retention, and escrow requirements were imposed on the registrars as terms and conditions of their accreditation to sell domain name registrations. Privacy advocates and civil liberties experts cried foul and demanded privacy and obscurity through proxy services. This standoff with law enforcement and intellectual property stakeholders on one side and civil liberties advocates on the other went on for roughly 14 years during which time the quality of the data in the directory decreased, and cybercriminals put inaccurate data in the registry (e.g., registering as Mickey Mouse or fraudulently impersonating legitimate trademark owners, such as Facebook).

---

[105] Affirmation of Commitments by the United States Department of Commerce and the Internet Corporation for Assigned Names and Numbers https://www.icann.org/resources/pages/affirmation-of-commitments-2009-09-30-en

In 2013, the new CEO of ICANN, in consultation with the board of ICANN, established an Expert Working Group to find a resolution to this standoff and to improve accuracy in the system while still providing for privacy. Recommendations resulted, but it remains to be seen whether they will be implemented. Issues surrounding the directory include the following:

- Because domain name registration is not something that the average consumer understands, it is doubtful that the average registrant realizes the uses and disclosures of registration information.
- Law enforcement officials obtain access informally over public networks to address and telephone information that they cannot get without a warrant or informally from similar systems such as cellphone directories or Internet Service Providers (ISPs).
- There is a wide variation in the application and enforcement of data protection law to directory information. The Article 29 Data Protection Working Party has written to ICANN repeatedly urging them to address privacy issues, state the purpose of the directory, and enforce privacy laws, but so far to no avail.
- There are now data escrow requirements in the Registrars Accreditation Agreement that go much farther than the data required for WHOIS. The agreement requires that registrars retain, for a period of 18 months after their last transaction with a domain name registrant, a broad range of information, including banking information and metadata. These requirements are considered unconstitutional by the European Data Protection Supervisor following the recent European Court of Justice decision which threw out the Data Retention Directive in the EU. Prior to that, the Article 29 Data Protection Working Party had written to ICANN informing them that Europe's 28 data protection authorities found the requirement to release personal data to the WHOIS unacceptable and that escrowing data for law enforcement violated data protection law. All European registrars needed a "waiver" of these contract requirements, which was a concession made by ICANN to the reality of data protection law.

The domain name registration system is an example of a data collection and disclosure requirements that grew through significant "function creep". Currently, data is accessed and reprocessed by a number of "value added" information service providers that provide trademark monitoring, brand protection, and WHOWAS services (i.e., who owned certain domain names). Trademark owners protect new creations (e.g., movies, clothing names, or food products) by purchasing names from existing owners. Internet search engines are mined to see what names are "hot" and domain squatters attempt to register trendy names first. None of this was predicted by early Internet pioneers who developed the first systems, but it has proven hard to quell the appetite for more uses of this information once the directory existed. To further complicate the arguments, cybercriminals and spammers use automated tools to prey on registrants, and companies and governments hire cybersecurity operations companies to police this abuse and remove miscreants.

In its final report in June 2014, the Experts Working Group at ICANN listed 16 "permissible purposes" for directory information, and stated in a principle that ICANN must allow for the development of new permissible purposes as the Internet DNS evolves further. This is of course the direct opposite of limitation of purpose and proportionality, key principles of the European Data Protection Directive and replacement regulation, under consideration at the present time. It appears that ICANN is on a collision course with data protection authorities, but this may be a slow crash as complaints from citizens are anticipated to trigger the court decisions.

In the meantime, the Council of Europe independently developed a paper on ICANN and human rights[106]. In this document, the authors refer to a recent report of the UN Human Rights Council entitled *Privacy in the Digital Age*[107], and express the view that global opinion was crystalizing around the idea that privacy was extremely important and ICANN would not be able to continue to ignore the human rights issues surrounding WHOIS.

Conclusions

- ICANN is headquartered in California, and some allege that California law respecting corporations strictly enjoins the board to protect ICANN from liability. This legal responsibility appears to be at cross-purposes with accepting the public policy obligations to respect privacy FIPs. Without getting into a legal debate about California corporate law, it is an important lesson that organizations set up to perform public policy functions should not have corporate structures or reside in jurisdictions that cause them to operate at cross-purposes to the rights of individuals.
- It is more difficult to stop providing personal data once companies that mine the data have built successful businesses with the information or once others rely on the data for their own purposes. Entrenched interests are hard to dislodge.
- Representation at multi-stakeholder organizations engaged in data sharing activities would be improved if it included data protection authorities and constitutional experts, particularly where governments are not required to sign on to policy requirements, and therefore the usual checks and balances are not in place. Governments pushed ICANN to make personal data public while demanding escrow for law enforcement purposes.
- The ICANN domain registration problem is complex, with many different players and with government agencies potentially on different sides from each other. Different parts of the same government can have different views, something familiar at any governmental level. However, in this instance, a private sector organization that is supposed to listen to its stakeholders in a bottom-up multi-stakeholder process also has to contend with governments from around the world making demands as governments, without any regulatory action on their part and thus potentially without going through their own interdepartmental processes to secure consensus.
- The clash between Internet governance and data protection controls is yet to take place, and the results are hard to predict.
- Many of the difficulties arise from the unprecedented, yet important, role of ICANN as a global multi-stakeholder body created to take action quickly on a rapidly growing Internet. It is quite possible that data sharing issues will arise in similar complex circumstances in which government roles will be limited, and others will have a greater voice in decision-making. The peculiar dynamics of ICANN and the Internet may make its data sharing issues poor examples for drawing lessons for more traditional data

---

[106] Zalnieriute, M. & Schneider, T. 2014. *ICANN's procedures and policies in the light of human rights, fundamental freedoms and democratic values*, DGI (2014)12. Strasbourg, France: Council of Europe. https://duckduckgo.com/l/?kh=-1&uddg=http%3A%2F%2Fwww.coe.int%2Ft%2Finformationsociety%2Fsource%2FDGI(2014)12E%2520ICANN-PoliciesProcedures(16June2014).pdf.

[107] Office of the UN High Commissioner for Human Rights, *The Right to Privacy in the Digital Age,* (2013). http://www.ohchr.org/EN/Issues/DigitalAge/Pages/DigitalAgeIndex.aspx

sharing activities in settings where there is clear political and other accountability. However, the importance of the Internet makes it hard to ignore.

- ICANN is an example of a new form of international governance structure, the "multi-stakeholder model". How ICANN reaches public policy decisions may become more important both for the decisions and the model of decision-making. Given that joint private/public sector data sharing initiatives have been proposed in some jurisdictions (e.g., U.K., Canada), it may be useful to examine the governance structures of not-for-profits.
- Transparency is always desirable, but transparency is not sufficient to make sure that privacy will be adequately represented. Someone must actively and effectively represent privacy.

7. U.K.: Joined-Up Government

- **WHO:** Following the election of the Labour Party government in 1997, the initiative was led by the Cabinet Office and the civil service with inclusion of local authorities

- **WHAT:** Harnessing the IT advantage presented by computing power and the Internet to integrate government services more completely and share information.

- **WHERE:** U.K. (the term was subsequently picked up by other countries)

- **WHY:** Primary stated purpose was to tackle persistent problems, notably crime, drugs and social exclusion, although there was recognition that the information society and global trade were having serious negative impacts on employment, particularly among blue collar workers.

- **WHEN:** Announced in 1997, trials in place by 2000, notable academic conference held October 2001 (i.e., British Academy: Joined-up Government). Expression appears to have fallen out of favour with the change in government, but the initiative is not dead, it has been revived most recently in the government response to the Law Commission report on data sharing tabled in July 2014.

- **HOW:** Joined-up government, as originally proposed, linked otherwise separate data systems, and as such was a classic "breaking down the silos" initiative. Now the system is usually referred to as "data sharing".

The U.K. government has tried to do "joined-up government", or provide the government with extensive data sharing powers and technical ability, for many years. It has basically been underway since 1997, but in the last decade there have been three waves, as described by Dr. Chris Pounder in his Amberhawk blog:

> The Government tried in 2006 with the Identity Card Act to permit general public sector access to the Identity Card database in order to help deliver efficient and effective public services. This was followed with wide data sharing powers in the Coroners and Justice Bill in 2008; after considerable

> opposition in the House of Lords, these were replaced by the data sharing code of practice provisions (which we all love). Third time round has happened with these proposals.[108]

Pounder concludes that the Cabinet Office, after holding separate meetings with stakeholders over the past year to consult on its data sharing plans, has decided to shelve the report of the Law Commission.

The Law Commission did extensive public consultations on data sharing in 2013, and released its final report to parliament in July 2014.[109] A press release[110] on July 11 sums up the situation rather well:

> Data sharing affects us all. Public bodies report that they cannot always share the data they need to share and, as a result, miss out on opportunities to provide better services to citizens. At the same time, the protection of privacy is fundamental to any data sharing regime. The law surrounding data sharing is complex. Powers to share data are scattered across a very large number of statutes and may be set out expressly or implied. In addition, there are common law powers.
>
> In this scoping project we considered the following questions:
>
> - Are there hurdles to effective data sharing between public bodies (including private bodies engaged in public service delivery)?
> - Are those hurdles inappropriate?
> - How far do problems in data sharing stem from the law?
> - How far do problems in data sharing stem from other causes, such as a lack of training or guidance, organisational incentives and disincentives?
> - Would law reform solve or mitigate the problems?
>
> We published our report, including our analysis of consultation responses on 11 July 2014. We made three recommendations.
>
> We recommend that a full law reform project should be carried out in order to create a principled and clear legal structure for data sharing, which will meet the needs of society. These needs include efficient and effective government, the delivery of public services and the protection of privacy. Data sharing law must accord with emerging European law and cope with technological advances. The project should include work to map, modernise, simplify and clarify the statutory provisions that permit and control data sharing and review the common law.
>
> The scope of the review should extend beyond data sharing between public bodies to the disclosure of information between public bodies and other organisations carrying out public functions.

---

[108] Push for new data sharing powers as Law Commission's data sharing report is shelved, http://amberhawk.typepad.com/amberhawk/.
[109] The Law Commission (Law Com No 351) *Data Sharing Between Public Bodies: A Scoping Report.* Presented to UK Parliament 9/10/2014. http://lawcommission.justice.gov.uk/docs/lc351_data-sharing.pdf.
[110] http://lawcommission.justice.gov.uk/news/2842.htm

> The project should be conducted on a tripartite basis by the Law Commission of England and Wales, together with the Scottish Law Commission and the Northern Ireland Law Commission.
>
> We consider that the project could usefully include consideration of the functions of the Information Commissioner in relation to data sharing, including the Commissioner's enforcement role. The work of other bodies providing advice and guidance should be explored to improve the consistent application of data sharing law across government and in public service delivery more widely.
>
> The investigation should also include consideration of "soft law" solutions such as codes of practice, as well as advice and guidance, training of staff, and ways of sharing best practice in the management of data sharing between public bodies.[111]

The consultation paper is available on the website[112], and many organizations published comments on the paper. The U.K. government released a paper with policy options on July 28, 2014, and the options look familiar.[113] The name of the initiative, however, is more in keeping with the discourse surrounding big data, as the services are now called Tailored Public Services.

The history of joined-up government initiatives in the U.K. remains instructive.

Dr. Perri 6 has written extensively about the earlier (circa 2000) joined-up government initiative in the U.K. in comparison with other countries, so it is useful to examine his definitions:

> Coordination: the development of ideas …about joint and holistic working, joint information systems, dialogue between agencies, processes of planning, and making decisions.
>
> Integration: the actual execution or implementation of the products of coordination, through the development of common organizational structures and merged professional practices and interventions.
>
> Joined-up government refers to consistency between the organizational arrangements of programs, policies, or agencies, which may enable them to collaborate.
>
> Holistic government is defined as the altogether more demanding business of starting with clear and mutually reinforcing sets of objectives framed in terms of outcomes and then working back from there to identify a set of instruments which have the same relationship to one another to achieve those outcomes. (p. 106). [114]

As can be seen from these definitions, the concept of joined-up government is not quite as simple as the phrase implies. In the early period of joined-up government, the government attempted to achieve common goals and integrate services. According to Dr. 6, the most successful trials in Europe related to "one stop shopping" efforts, where citizens could go to one government outlet to obtain the most common services. As was noted in previous examples, in Australia this became a

---

[111] http://lawcommission.justice.gov.uk/publications/2811.htm
[112] http://lawcommission.justice.gov.uk/docs/cp214_data-sharing.pdf.
[113] https://docs.google.com/document/d/1g6kpiRUpgECnR2IXCuP0O1_VmuMMBgbD-oCmQI4wHVE/edit?pli=1
[114] 6, Perri. *Joined-Up Government in the Western World in Comparative Perspective: A Preliminary Literature Review and Exploration in the Journal of Public Administration Research and Theory*, Journal of Public Administration Research and Theory: J-PART Oxford, United Kingdom: Oxford University Press) 14: pp103–138. doi:10.1093/jopart/muh006, http://jpart.oxfordjournals.org/content/14/1/103.abstract.

separate operating agency, Centrelink, and Service Canada was formed to fill this role in Canada, although Service Canada never achieved separate agency status.

Qualitative research done by Dr. 6 and commissioned by the Cabinet Office sought the reaction of client groups to the government proposals in 2001. Research involving in-depth interviews of clients is relatively rare, and this is a small sample size, but it is nevertheless interesting and revealing. Dr. 6 interviewed the following subjects in focus groups: income support claimants, self-employed men, school leavers in low paid or temp work, female recent immigrants and granted asylum, recently retired people, and regular drivers.

The questions started with what the interviewees understood of data sharing and data controllers, and went on to perceived benefits and risks. Dr. 6 identified the following risk frames for viewing joined-up government: indignity, lack of control, injustice, inconvenience, and nothing to hide. Not surprisingly, the more vulnerable the individual was in their social position and employment, the more likely they were to be at the indignity end of this continuum. He questions, however, the mobility of individuals from frame to frame in terms of how they perceive privacy risk, and this remains a relevant question today, particularly as the baby boomers enter retirement. How will they view the matter of privacy as they reach the age of vulnerability?

In 2003, the New Zealand Data Commissioner's Office hosted a workshop on experience and best practice with PIAs in Auckland, New Zealand. Independent contractors present at the workshop discussed "joined-up justice" PIAs in no fewer than three jurisdictions. The contractors reported, without revealing any confidential details, having serious issues with the legal and constitutional complexities of such systems. It is not, therefore, surprising that fulfillment of the promise of joined-up government was slow, and the term has more or less been dropped. The legal complexities described in the U.K. Law Commission report sound very similar to the ones discussed in Auckland a decade earlier.

Dr. Ross Anderson of Cambridge University led a team from the Foundation for Information Policy Research (FIPR) to produce the report *Database State* in 2009 under contract with the Rowntree Trust[115]. It followed the loss, and resultant scandal, in October 2007 of 25 million child-benefit records, and in it he describes the failures of joined-up government as well as the conflicts that inevitably arise:

> The (conflicting) ambitions to make government 'joined-up' and to make every public service available online date back to the dotcom boom era. Government IT spending increased significantly after that boom ended, with the launch of projects such as the NHS National Programme for IT. But government found targets easier to set than to achieve. As IT projects continued to fall far short of expectations, government focussed – with the McCartney 2001 review, the formation of the Office of Government Commerce and its Gateway process – on project management, procurement and relations with suppliers. The 2005 Transformational Government IT strategy[6] promised citizens choice and personalization in their interactions with government. However, this was to be based on centralised databases and data sharing across traditional provider and departmental boundaries. At its heart lay not people, but great collections of data about people.

[115] The Rowntree Trust was started by Joseph Rowntree (of Rowntree chocolates fame), who was a Quaker and committed to issues of social justice. See http://www.jrct.org.uk/.

> Meanwhile, two different faces of government were being joined up. One is the public services agenda, which formalises our social compassion. It speaks of customers and choice, cares for vulnerable children, provides health and education, keeps the streets clean and generally seeks to please. The other is the enforcing state, in constant conflict with those who break laws or ignore regulations. It seeks to exercise coercive control and speaks of enemies, targets, suspects and criminals.[116] (p.9)

Anderson analyzed 46 of the key databases in the U.K. using a traffic light rating system for their compliance with privacy and human rights law, including intrusion. Only six received a green light. The evidence in 2009 found that the U.K. tended toward centralized systems where access may be shared, but the actual databases are still mostly in silos.

There are many interesting observations in the Law Commission Report, as it undertook extensive consultations and interviews with citizens, data users, and civil society. Let us focus on only one, the "Troubled Families" initiative. Because this project links data about families at risk (e.g., criminal records, health records and social services) it may be of interest in the provincial context in Canada. It also appears to be a revisiting of the U.K. Children's Services initiative, which is described in the next case study.

The Law Commission notes that the Department of Work and Pensions, the taxation department, and the Department for Communities and Local Government all shared data. The program was premised on the estimate that:

> 120,000 troubled families cost the taxpayer 9 billion pounds annually – 75,000 pounds per family per year – of which 8 billion are spent purely in reacting to the families' problems, rather than improving their outcomes. The first phase of the programme sought to identity target families using four cumulative criteria: high levels of anti-social behaviour or youth crime, children excluded from or not attending school, adults claiming out-of-work benefits and a fourth criterion set by local authorities based on "local intelligence" as to the most significant problems in their localities.
>
> 10.4 The data necessary for this exercise are held across a multiplicity of different local and central public sector agencies. A corresponding multiplicity of different data sharing agreements were required with different parts of government. The process was complex, produced patchy results and incurred high transaction costs. Some data sharing was not possible, such as identifying families with priority health problems, as no legal gateway could be found or devised. (p.163)

In the next case study problems will be identified with respect to social services data sharing which had stopped an earlier initiative targeted at protecting children for many of the same reasons. It is noteworthy that the Association of Police Chiefs and the Information Commissioner actually challenged the practice of sharing police data in bulk in 2012, and went on to work together to develop guidance for police.

The Information Commissioner presented a response[117] to the consultation, and notes that the Information Commissioner's Office is unaware of any research on public trust, but that it appears

---

[116] http://www.jrrt.org.uk/publications/database-state-full-report.

[117] http://ico.org.uk/about_us/consultations/~/media/documents/consultation_responses/ICO-response-to-Law-Commission-Data-Sharing-consultation.pdf.

that the public is very uncertain as to the degree of control they can exercise over their data when shared:

> Organisations should explain to the public as clearly as possible whether the sharing of their personal data is voluntary or mandatory- this is an important element of the 'fairness' requirement of data protection law. We would encourage the Law Commission to give due consideration to [the] extent to which individuals should be able to exercise control over the sharing of their personal data. We suspect that this is a major source of uncertainty amongst policy makers and practitioners. (p.9)

The Information Commissioner also noted the tension between the need to keep personal data secure and the desire to share it as well as the different levels of security that resulted with data shared between different organizations.

Conclusions

- Central databases may be more prevalent in countries where power and administration are centralized and not shared with provincial governments.
- While there was a first wave of enthusiasm for joined-up government both during and following the dotcom boom, enthusiasm waned as governments realized how complex the projects are to bring to fruition. Failures were numerous, but the desire to reduce government costs and predict risk continues to drive data sharing initiatives.
- Privacy and human rights concerns, including intrusion and discrimination, are serious impediments to joined-up government, although they are far from the only impediments. While few cases have been litigated, the risks are real and difficult to manage in systems procedures, short of not collecting and sharing the personal data.
- In the early attempts at joined-up government, funded U.K. advocacy groups exposed issues and mounted campaigns for change. The Rowntree Trust, the FIPR, Liberty, Privacy International, and Statewatch all intervened on the much later U.K. Law Commission consultations, although it remains to be seen what will happen with this initiative. Canada does not have as many trusts and foundations as the U.S. and the U.K., but there are donors and the possibility of advocacy groups becoming more active should not be discounted. It only takes a few people to start a dynamic organization.
- In the latest round of response to the U.K. data sharing proposals and consultations, an organization called Involve coordinates the drafting of documents for civil society. Using social media and open document platforms, Involve opened up the process of consultations remarkably.[118] While it remains to be seen whether Involve's leadership will produce better outcomes than previous efforts to reach compromise on government proposals, it is a strikingly interesting and novel development. There does not appear to be any Canadian equivalent.

8. U.K.: Children's Services

- **WHO:** Department for Education and Skills (DfES), local social services authorities, National Health Service (NHS), and police services.

---

[118] http://datasharing.org.uk/whos-involved/.

- **WHAT:** Databases relating to children across social services, education, crime and health, with a central register (ISA). Patterned on the NHS electronic records model.

- **WHERE:** U.K., excluding Scotland.

- **WHY:** Early intervention in the lives of at-risk children, to deter child abuse (child protection) and criminal activity (risk prevention or general social benefit).

- **WHEN:** Green paper *Every Child Matters* published 2003; analysis by FIPR for the Information Commissioner published 2006; and project appears to be ongoing.

- **HOW:** A series of trials developed multi-agency information sharing.[119] A university consortium developed a toolkit and recommended software and platforms.

This analysis relies heavily on the report that the FIPR completed for the Information Commissioner in 2006.[120]. The U.K. government, in keeping with trends common in European and western democracies, was shifting from a child protection model of social services responsive to reports of abuse to a "prevention" model. Prevention models use risk factors to identify children likely to be at risk in order to establish surveillance, and involve them in activities less likely to lead to crime and under-achievement.

Child abuse reports triggered the change in approach as well. The case that attracted tremendous attention was the death of Victoria Climbie, a child who died horrifically in the care of relations acting as foster parents even though social services should have been aware of issues. Parliament requested a full independent inquiry led by Lord Lambey that detailed necessary changes in the child protection system.[121] He recommended the government investigate the possibility of a national database on children. However, much of the report, which is difficult to read as it details the tragedy of the failure of social services to protect this child, focuses on the lack of accountability of social services staff, the tendency of managers to distance themselves from the day to day affairs of their client populations, and the utter failure to communicate effectively. Anderson et al. are skeptical of the recommendations of big systems to solve human problems:

> If one of the core problems in accurately identifying children who are suffering, or are at risk of suffering significant harm, is the level of professional expertise in understanding data (rather than a lack of data per se), then providing more data does not seem to be the most obvious strategy for improving practice. In fact it may be counter-productive. If there is more data, time will be spent on absorbing it rather than acting upon existing data. Additionally, important data may be hidden below insignificant data – this problem is well understood by those responsible for running criminal investigations, particularly those in real time (such as kidnaps), with which section 47 cases may be compared.[122]

---

[119] See http://www.fame-uk.org/
[120] Foundation for Information Policy Research. *Children's Databases: A Report for the Information Commissioner* (2006). http://www.cl.cam.ac.uk/~rja14/Papers/kids.pdf.
[121] Laming, W., The Victoria Climbie Inquiry (2003), London, The Stationery Office, https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/273183/5730.pdf.
[122] http://www.cl.cam.ac.uk/~rja14/Papers/kids.pdf.

According to the report, there were many key data collection databases:

Social Services

CAF: the Common Assessment Framework to be completed by any professional who decides that a child has additional needs that require the involvement of more than one service. It is a wide-ranging set of data covering every aspect of a child's health and development, including details about the parents and siblings.

ISA or IS: Information Sharing (and Assessment) Index, containing basic details of all children in England, including all professionals in contact with them and their contact details.

ICS: a system for children's social services that will include the case records of all children known to social workers. The extent to which information on this database will be linked to the systems in health, education, and criminal justice is not yet clear.

Education

CCIS: Connexions, a database run by local education and skills authorities mandated through learning and skills councils, authorized by the Learning and Skills Act of 2000. The plan is to link these databases, so that detailed client information (all children over age 13) is shared nationally through the Connexions Customer Information System.

APIR: Assessment, Planning, Implementation and Review, a database compiled once a child is referred for counseling to a Personal Advisor (PA), established through the Connexions system. This is an electronic system, under the control of the PAs, who decide what parts of the record to share with other agencies.

NPD: National Pupil Database, operated by the Department for Education and Skills, accessible by small numbers of local authorities.

Police:

ASSET: structured assessment tools to profile young offenders.

ONSET: structured assessment tools to profile youth at risk.

RYOGENS: Reducing Youth Offending Generic National Solution, a centrally-managed database accessed by practitioners in the partner local authorities via the Internet. It allows workers in social services, education, health and youth justice teams to share details of minor concerns they hold about children, based upon factors derived from ONSET and the Department of Health's Framework for the Assessment of Children in Need and their Families.[123]

This all sounds logical enough, but the number of separate databases maintained by different organizations is a bit overwhelming. Even more overwhelming is the list of the factors, with their troubling privacy, accuracy, and profiling consequences, included in just one of the databases: victim or perpetrator of bullying/harassment, negative home influence on education, poor school

[123] http://www.cl.cam.ac.uk/~rja14/Papers/kids.pdf.

attendance, parental substance abuse, dangerous behavior, social isolation, self-harm, and many others that involve highly subjective judgment.

The FIPR report comprehensively assesses the various aspects and risks of this proposed interconnection of a myriad of databases. The report provided a detailed legal/regulatory analysis of the data sharing as it existed at the time, and whether in fact it was legally permissible to collect, use, and disclose the information (see their Chapter 7). This analysis is omitted from this report in the interests of space, but it is of interest to those wishing to examine similar initiatives here in Canada, although the legal framework is obviously quite different.

The FIPR report offered three strategies for the Information Commissioner, basically along the Goldilocks principle:

> The first strategy requires minimal action and entails the Commissioner simply following previous UK practice – issuing enforcement notices for the most serious problems but generally hoping to encourage departments to issue regulations and guidance that formalise existing and planned practices.
>
> In the second possible strategy, the Commissioner seeks to engage government and the public in a debate about the right balance between privacy and child welfare, and to influence not just the shape of regulation but the design of the next generation of systems.
>
> In the third possible strategy, the Commissioner would take an even more active role by challenging a number of existing UK practices which would not be legal in other European countries. The Commissioner could also challenge the Government to provide evidence of benefit to balance the harm done by privacy intrusions, and rule against such intrusions where evidence could not be produced.[124]

Other U.K. scholars wrote about the children's database project and the overall joined-up government proposals, notably Charles Raab, Christine Bellamy, and Perri 6. Dr. 6 has also published a detailed analysis of the ethics of risk management profiling as it applies to vulnerable populations, which, while somewhat beyond the scope of this report, does speak to privacy concerns and risks inherent in the new data mining capabilities. Some relevant material is included in the bibliography.

As was noted in the previous case, the Information Commissioner's Office weighed in to challenge bulk sharing of police data. Aspects of the children's database were scrapped, but it is likely that some aspects of the program will be revisited in today's reactivation of data sharing. If the Cabinet Office proceeds with more liberal data sharing provisions in legislation, the obstacles to the earlier initiatives may partially be removed.

Conclusions

- Tragic events can propel social policy in ways that may skew the emphasis on procedures. In the U.S. in particular, privacy has benefited from so-called "horror

[124] http://www.cl.cam.ac.uk/~rja14/Papers/kids.pdf, at p. 130.

stories" that resulted in the enactment of privacy legislation at the state and federal levels. As is clear from the UK example, horror stories can cut both ways.[125]

- The FIPR report identifies a fundamental failure to recognize the "messiness" of social service work; by its very nature it is not always possible to predict abuse. Computer systems examining data are not likely to overcome a fundamental human problem.
- Over-reporting of risk indicators can become a problem in systems designed as early detection systems. In this instance, after a high profile case, it is likely that anyone involved in child welfare would over-report rather than risk missing a tragic situation. This occurred with do-not-fly lists. Although data collected by FINTRAC is not readily available, the "suspicious transactions" which must be reported, subject to criminal penalties for failure to report, likely tend towards over-reporting. The Privacy Commissioner of Canada noted this in the FINTRAC audit report in 2013.[126]
- It is important to keep in focus the fact that intervention, whether to detect fraud, child abuse, or disease, has to be done by humans who evaluate the data and determine that scarce resources should be spent on this or that case. Data analysis, even if computer assisted with the latest data analytics, still largely depends on the humans who input and make use of it. A system that produces more "hits" than a staff or budget can review and investigate may create more horror stories and demands for accountability than the bureaucracy and the political level of government can address. The tradeoffs here are difficult and delicate.
- Academics and civil society played a key role on this issue. The importance of FIPR's work here is already clear. Privacy International held a meeting on this topic, bringing together academics across a broad range of disciplines, including computer scientists and social workers. Some of the activities that surrounded this initiative in the U.K. will be described in chapter 7 of this report.
- The Caldicott Review of 2013[127] cited the FIPR report, and certainly discussed the Information Commissioner's Office guidance as well. It seems important to establish a volume of work on the topic, from various quarters in society, in order to make progress.

9. U.S.: Internal Revenue Service Sharing Tax Data with States

- **WHO:** Internal Revenue Service (IRS)
- **WHAT:** Sharing of income tax records with state income tax authorities

---

[125] Canada of course had a similar situation recently, when the federal government used the unfortunate suicide of a victim of cyber-bullying as a policy rationale for drafting brief criminal code amendments on cyber-bullying, and attaching them to an old piece of draft legislation on law enforcement access to ISP and telecom data, now passed by the legislature. The outgoing Ontario Privacy Commissioner was vocal about what was wrong with that initiative. http://www.cbc.ca/news/politics/cyberbullying-bill-surveillance-powers-alarm-ontario-privacy-watchdog-1.2649523. Even the mother of one of the cyber-bullying victims spoke out to say that the harms of cyber-bullying could not justify the intrusion into everyone's privacy, but to no avail. http://www.cbc.ca/news/politics/cyberbullying-victims-parents-divided-over-privacy-concerns-in-online-bill-1.2641104.

[126] https://www.priv.gc.ca/information/pub/ar-vr/ar-vr_fintrac_2013_e.pdf, at p. 23-25.

[127] Information: To share or not to share? The Information Governance Review (March 2013), https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/192572/2900774_InfoGovernance_accv2.pdf.

- **WHERE:** U.S.

- **WHY:** Sharing supports the overlapping missions of the IRS and individual states with respect to the collection of taxes

- **WHEN:** Ongoing

- **HOW:** Through matching agreements overseen by each agency's Data Integrity Board

The principal function of the IRS in the U.S. is the collection of business and personal income taxes. Most states and some local governments also impose income taxes and require taxpayers to file state income tax returns using forms that differ from the federal income tax returns. IRS shares tax returns with hundreds of federal, state, and local agencies for a variety of purposes specified by law. The focus here is on the IRS's sharing of personal tax information with state agencies, but the procedures described here are common to sharing with other organizations.

A federal statute provides that tax returns are confidential.[128] The same statute provides numerous exceptions, including one that permits the sharing of tax returns with state tax officials.[129] The statute requires a written request from the head of the state agency.[130] This is the first in a series of statutory and administrative requirements imposed on state recipients of federal tax returns.

Another provision of the tax confidentiality section establishes more detailed conditions for requesting tax returns. These include:

- establishing and maintaining a permanent system of standardized records with respect to any request, the reason for the request, and the date of the request made and of any disclosure of return or return information made;
- establishing and maintaining a secure area for storage of the returns;
- restricting access to the returns only to persons whose duties or responsibilities require access and to whom disclosure may be made;
- providing other safeguards that the Secretary determines to be necessary or appropriate to protect the confidentiality of the returns;
- furnishing a report to the Secretary[131] describing the procedures established and utilized by the State for ensuring the confidentiality of returns; and
- upon completion of use of returns, providing for the return to the IRS, erasure, or destruction of the returns.[132]

Supplementing the broad statutory requirements for obtaining federal tax returns is IRS *Publication 1075*, a 173-page document with considerably more detailed specification of the security

---

[128] 26 U.S.C. § 6103, http://www.law.cornell.edu/uscode/text/26/6103.
[129] Id. at § 6103(d). The law provides for sharing of return information with other State officials, but the discussion here focuses only on tax officials.
[130] Id.
[131] Secretary of the Treasury. The IRS is a component of the Department of the Treasury.
[132] 26 U.S.C. § 6103(p)(4), http://www.law.cornell.edu/uscode/text/26/6103.

requirements.[133] The publication is the product of the IRS Office of Safeguards, an office specifically devoted to ensuring that federal, state and local agencies receiving federal tax information "protect it as if the information remained in IRS's hands."[134]

Publication 1075 describes requirements for the preparation of the state and approval by the IRS of an annual Safeguard Security Report. In addition, IRS requires advance notification by the state of the use of these facilities or activities involving the use of tax returns:

- cloud computing;
- consolidated data center;
- contractor access;
- data warehouse processing;
- non-agency-owned information systems;
- tax modeling;
- test environment; and
- virtualization of IT systems.

IRS took its lengthy computer security framework in *Publication1075* from guidelines specified in National Institute of Standards and Technology's (NIST) SP 800-30 Revision 1, *Guide for Conducting Risk Assessments*,[135] and NIST SP 800-53 Revision 4, *Security and Privacy Controls for Federal Information Systems and Organizations*.[136] NIST is a component of the U.S. Department of Commerce and its mission includes the development of standards.

The Office of Safeguards is itself subject to audit by the Treasury Inspector General for Tax Administration.[137] As with other federal agencies, oversight by the government's auditors at the Government Accountability Office and oversight by the Congress also provide accountability. There is little public awareness of tax information sharing by the IRS.

Conclusions

The extent to which the IRS and its Office of Safeguards successfully carries out its mission to safeguard the security of tax information that it shares with the States is beyond the scope of this report. However, the structure and extent of the controls are impressive.

- When the stakes – be it personal data or agency turf – are high enough, and the resources are available, it is possible to develop a comprehensive program to oversee the confidentiality of shared information.

---

[133] Internal Revenue Service, *Tax Information Security Guidelines for Federal, State and Local Agencies* (Publication 1075), http://www.irs.gov/file_source/pub/irs-pdf/p1075.pdf.
[134] http://www.irs.gov/uac/Safeguards-Program.
[135] csrc.nist.gov/publications/nistpubs/800-30-rev1/sp800_30_r1.pdf.
[136] nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r4.pdf.
[137] See, e.g., *While Effective Actions Have Been Taken to Address Previously Reported Weaknesses in the Protection of Federal Tax Information at State Government Agencies, Additional Improvements Are Needed* (2009), Reference Number: 2010-20-003, http://www.treasury.gov/tigta/auditreports/2010reports/201020003fr.pdf.

- Requiring those who want access to personal information to sign agreements establishing the terms of data use and data security will work when the interest in data sharing is high. It may be that the revenues available as a result of the data sharing are high enough to support extensive security in order to obtain the revenues.
- With respect to computer security requirements, it is not necessary to reinvent the wheel, but computer security standards established by respected external organizations (e.g., government) can be referenced and used.
- It is possible to control data sharing activities that make use of leading edge technologies (e.g., cloud computing) and sophisticated management facilities (e.g., consolidated data centers).
- The IRS data controls developed without any significant attention or pressure from public interest groups. The IRS had sufficient incentive to protect its turf and its data while under political and policy pressure to share data. Those who wanted the data could not object to privacy and security rules. In this case, the bureaucratic interests of the IRS and the privacy/security interests of IRS data subjects overlapped. That is not always the case.

10. U.S.: *Computer Matching and Privacy Protection Act*

- **WHO:** Federal agencies
- **WHAT:** Computerized comparison of automated records systems containing personal information
- **WHERE:** U.S.
- **WHY:** Establishing or verifying eligibility for government programs or recouping payments or delinquent debts
- **WHEN:** 1977 – ongoing
- **HOW:** Through matching agreements overseen by each agency's Data Integrity Board

History

Computer matching began in the U.S. as an administrative activity and policy controversy in the late 1970s, just a few years after the U.S. passed the first national privacy law of the Fair Information Practices era. The *Privacy Act of 1974*[138] was just a few years old when computer matching capabilities developed and raised difficult questions about the Act's standards for controlling disclosures between agencies for disparate benefit programs. In its original form, computer matching involved the comparison of computer tapes of different programs to determine if any individual was a beneficiary of both. An early match compared the federal payroll in the Washington, DC, area with

[138] 5 U.S.C. § 552a, http://www.law.cornell.edu/uscode/text/5/552a.

local welfare rolls. The presumption was no one could be on the federal payroll and lawfully receive welfare.[139]

The legal question was whether it was compatible with the purpose of federal payroll programs to use those records to find individuals ineligible for welfare. Arguments raged on both sides, but the political attractiveness of finding welfare "cheaters" combined with budgetary pressures and subsequent legislation supporting matching overcame the original legal and policy objections. Privacy eventually staged a comeback of sorts with the passage of the *Computer Matching and Privacy Protection Act of 1988*.[140]

The matching law established "procedural" rules for the approval of computer matches, but did not set standards governing when data sharing was permissible. Each agency involved in a computer match needed approval of its formal matching agreements from its own internal Data Integrity Board. However, partly because of the lack of outside involvement and internal conflicts of interest, the board had no real interest in constraining matching. In some agencies, the boards never actually met, operating instead by passing paper back and forth between members. Nor did the boards try to expand their role in privacy to address other matters besides matching.[141] The internal administrative structure and economic test (i.e., "cost–effectiveness") in the *Computer Matching and Privacy Protection Act* did not appear to constrain matching in any significant way.[142]

Inconsistent administration of the Act's requirements, incomplete reporting, lack of rigor, and an absence of oversight contributed to the Act's failures. Nevertheless, the Act's administrative requirements, however inconsistently applied, and the lengthy process for approval were cited as barriers to matching.[143] It may be that the procedural requirements deterred short-term matching activities.

Further, changes in technology and administrative practices made the matching controls partly obsolete. Programs developed so-called "front-end verification" aimed at keeping ineligible individuals from enrolling in other government programs. Backend activities like computer matching lost some of their allure, although matching continues today.

Computer Matching and Due Process

An important element of the *Computer Matching and Privacy Protection Act of 1988* was the requirement that no agency involved in a computer match could take adverse action against the recipient of financial assistance unless the agency independently verifies the information and the affected individual receives notice of the finding as well as a timely opportunity to contest the findings. There is some reason to believe that the Act's due process requirements have been more successful than its

---

[139] The presumption turned out not to be true for a variety of reasons, including different time periods, small salaries and large families, and incorrect identity numbers. Agencies later learned how to avoid these mistakes made during early matching activities.
[140] Public Law 100-503, 102 Stat. 2507, gpo.gov/fdsys/pkg/STATUTE-102/pdf/STATUTE-102-Pg2507.pdf.
[141] Agencies later established privacy offices, sometimes at legislative direction and sometimes on their own initiative. However, the impetus for privacy offices was wholly unrelated to the Data Integrity Boards.
[142] The Matching Act specifically exempted many types of computer matching from regulation, including matching for criminal law enforcement, most tax purposes, and foreign counterintelligence purposes.
[143] Government Accountability Act, Computer Matching Act: OMB and Selected Agencies Need to Ensure Consistent Implementation (2014) (GAO-14-44), http://gao.gov/products/GAO-14-44

other provisions, and indeed have had widespread influence. A similar provision remains as a key element in the draft EU data protection regulation of 2013, and it was also present in the 1995 EU Directive as a prohibition on machine decision making.

Because computer matching is a defined and discrete activity, the law could readily require due process requirements before an agency could affect the rights, benefits, or privileges of an individual. However, when the silos between systems dissolve and record sharing between agencies or programs is no longer a discrete event, it may be harder to find a specific activity or step to which due process requirements can attach. Making sure that any program affecting individuals provides due process is not impossible or unfamiliar to government, but the importance of due process can be lost when agencies share record systems.

An example of how privacy can give way to overriding legislative directions comes from federal child support enforcement activities that began in earnest in the mid-1970s as the political flavor of the month. Any question whether disclosure by a federal agency to the federal child support enforcement agency was compatible with the purpose of the agency's programs was resolved when Congress passed a law directing each agency to disclose.[144]

The Act's attempt to impose a cost-effectiveness standard as a control appears to have failed because of a lack of standards and definitions. Those who promoted and used matching had little interest in demonstrating that the matching was both a financial success and better than alternative methods of preventing fraud, abuse, and waste.

What this limited history shows is that, under the right circumstances, political and other pressures to share records were able to readily overcome privacy objections. Support for the broad goals of computer matching – greater efficiency, reduced costs, and fraud prevention – are universal. A general privacy law, like the U.S. *Privacy Act of 1974*, can only withstand the pressure for so long. This was especially the case when the privacy side of the debate in the U.S. did not benefit from participation by a dedicated privacy official. Elected politicians faced the problem of appearing to be protecting "welfare cheaters". It took courage by a Senator and the lack of organized opposition to allow the *Computer Matching and Privacy Protection Act of 1988* to pass without opposition.

It was the case then as now that the U.S. lacks an independent privacy agency to provide general oversight or exert pressure. The Office of Management and Budget, which had responsibility to issue matching guidance, was not aggressive in directing or advising agencies. Privacy groups and stakeholders in programs subject to matching showed little interest. It may be telling that in a country like the U.S. where policy fights often end up in the courts there has been virtually no litigation over the computer matching parts of the *Privacy Act of 1974*.

It is also possible that the due process requirements in the *Computer Matching and Privacy Protection Act* addressed the more pressing unfairness problems that matching created for individuals. The importance of due process may be a more positive lesson to learn when data sharing affects individual entitlements. The absence of many computer matching horror stories may also have contributed to a lack of attention. U.S. privacy activities have been traditionally driven in significant

---

[144] 42 U.S.C.§§ 653, 653a, http://www.law.cornell.edu/uscode/text/42/653.

part by stories about injustice, harm resulting from specific data uses, and inappropriate applications of technology.

Computer matching today is not a pressing privacy issue in the U.S. The requirements of the *Computer Matching and Privacy Protection Act of 1988* appear to remain as a bothersome administrative deterrent to some matches. Many elements of the *Privacy Act of 1974* are technologically out of date, and that may be true as well for the matching provisions. There seems little interest in updating the law.

Conclusions

- The absence or presence of a high level data protection authority can contribute to the success or failure of privacy controls for computer matching, as well as other issues, of course.
- Depending on the specific activity, providing due process for individuals with respect to the use of their personal information may be more important than providing more narrowly focused privacy controls. Due process and privacy are not, however, mutually exclusive.
- Separate and internal privacy oversight entities within departments may not be successful if they have a narrow purpose and no external pressure or participation. Other evidence from the U.S. suggests that agency privacy offices can be useful, especially with legislative authorization and high-level agency support.
- Procedural controls over matching, requiring written agreements and internal approval, may be more effective at limiting matching than substantive controls (i.e., requiring proof of cost-effectiveness).
- Privacy controls based on specific technological implementations will become outdated if they are not adjusted to later development

11. U.S.: Department of Homeland Security Information Sharing and Safeguarding Strategy

- **WHO:** U.S. Department of Homeland Security (DHS)
- **WHAT:** Establishing the vision, mission, goals, and objectives for sharing and safeguarding information as well as managing the associated risks
- **WHERE:** U.S.
- **WHY:** DHS seeks to support its missions through sharing and safeguarding information
- **WHEN:** January 2013 - ongoing
- **HOW:** A common information sharing and safeguarding policy within the context of DHS's distributed homeland security architecture

The U.S. DHS is a large federal agency that is a complex amalgam of multiple agencies, missions, and programs. Components of DHS work with each other and with many other federal, state, local, and foreign government agencies. DHS shares information with private sector entities as well.

Data sharing is a major activity of the Department managed through a high level strategy,[145] an Information Sharing and Safeguarding Governance Board, and an Information Sharing Coordinating Council. The objective of the strategy is the establishment of a DHS Information Sharing Environment that will enable a comprehensive and streamlined ability to share and safeguard critical information across the Homeland Security Enterprise.

The high level attention paid to information sharing is evidence of both the importance of sharing to the agency and the commitment of management to sharing under the right terms and conditions. While privacy is not the only element of the information sharing strategy, it is one of the important elements. It is also the only aspect of the DHS strategy reviewed here.

The broad policy of the DHS Information Sharing Environment provides that DHS components, offices, and personnel must further share and safeguard information essential to the operational success of those tasked with the safety and security of the nation while maintaining appropriate privacy, civil rights, and civil liberties protections. An objective is the creation of a culture of information stewards to eliminate the divide between information "users" and information "owners" through a trusted risk management environment.

Noteworthy elements include:

- addressing privacy, civil rights, and civil liberties early in the planning of any new initiative;
- considering privacy, civil rights, and civil liberties in the common metadata tagging standards;
- ensuring all information sharing access agreements include privacy, civil rights, and civil liberties protections;
- coordinating information sharing access agreements with oversight offices; and
- having information sharing access agreement provisions for the conduct of privacy interests, civil rights, and civil liberties audits or compliance reviews.

Because DHS is a large enterprise, there are many layers to the management and operations of affecting data sharing. Another component is the DHS Data Framework, which it describes as a "scalable information technology program with built-in capabilities to support advanced data architecture and governance processes."[146] Development of the data framework is ongoing, and it is not possible at present to assess implementation specifics, compliance, or effectiveness.

For present purposes, what is important about the DHS data framework is the goal of alleviating mission limitations associated with stove-piped information technology systems. There are four elements for controlling data in the framework:

---

[145] U.S. Department of Homeland Security, DHS *Information Sharing and Safeguarding Strategy* (2013), http://www.dhs.gov/sites/default/files/publications/12-4466-dhs-information-sharing-and-safeguarding-strategy-01-30-13--fina%20%20%20.pdf.

[146] U.S. Department of Homeland Security, Privacy Impact Assessment for the DHS Data Framework (2013) (DHS/ALL/PIA-046), http://www.dhs.gov/sites/default/files/publications/privacy-pia-dhs-wide-dhsdataframework-11062013.pdf.

- user attributes identify characteristics about the user requesting access such as organization, clearance, and training;
- data tags label the data with the type of data involved, where the data originated, and when it was ingested;
- context combines what type of search and analysis can be conducted (i.e., function), with the purpose for which data can be used (i.e., authorized purpose); and
- dynamic access control policies evaluate user attributes, data tags, and context to grant or deny access to DHS data in the repository based on legal authorities and appropriate policies of the Department.

These elements will support access controls that include a dynamic access control mechanism that enhances privacy protections through definition and enforcement of who (i.e., user attributes) is allowed access to individual data elements (i.e., data tags) for particular purposes (i.e., context = purpose + function). In order for these controls to function: users requesting access to information must be described in a standard way through user attributes; source data must be defined in a standard way through data tagging; and applications must indicate for what purpose and how users will search the data through context.

This type of access control is more granular than the more familiar role-based access control system, which DHS is phasing out. Once in place, the new approach will allow for automatic evaluation of access requests and automated policy-based decisions to permit or deny access to information. Given the size of the department and the diversity of its operations and databases, the attraction of an automated system of controls is apparent.

There are clear costs and risks. For the system to work as planned, a great deal of coding is needed to identity individuals, to define their allowable activities, and to determine what are allowable uses and disclosures of data. Failure to establish sufficiently granular codes will either allow too much or too little access.

DHS plans to use tamper-resistant audit logs that will be used to assess both performance and compliance. The audit logs will capture successful and unsuccessful attempts to log in, to access information, as well as other meaningful user and system actions. The audit logs will contain the user ID and the query performed. The logs will allow audits of the control system by the DHS Privacy Office.

Conclusions

Few organizations are as large as the U.S. Department of Homeland Security, and even fewer will have the resources or resolve to establish high-level, comprehensive data sharing policies or the ability to implement them fully. It remains to be seen if the DHS data framework will be successful. However, many of the ideas that are part of the DHS system may have some applicability elsewhere. These include:

- a formal data sharing strategy rather than a series of uncoordinated policies;
- a high-level data sharing governance board rather than ad hoc or low-level data sharing decision making;
- addressing privacy early in planning rather than never or when it may be too late;
- use of information sharing agreements rather than informal arrangements;

- including in those agreements a role for a privacy oversight office rather than ignoring the possibility of oversight;
- more granular data access and use controls rather than a single access/no access decision;
- audit logs to support audits rather than no method for ensuring compliance and adjusting policies; and
- the use of technology and data tagging to control use and disclosure of personal information in a more granular way rather than role based access controls.

12. Denmark: E-Government Services

- **WHO:** Danish federal government in cooperation with state and municipal governments
- **WHAT:** E-government initiative setup to modernize services
- **WHERE:** Denmark
- **WHY:** Provision of citizen services online or "one-stop shopping"
- **WHEN:** 1996 - ongoing
- **HOW:** Secure communications are enabled by a digital signature system, and central services ensure easy access electronically to all levels of government, including municipal.

Denmark has been a leader in e-government for a number of years. It has a high level of broadband services and a high level of Internet use among the population. There are three components to the system:

- a citizen portal called "My Page" where citizens can access all their transactions with government, including municipal and housing[147];
- a secure email and archive system called e-Boks, which was set up through a public-private partnership and provides secure communications with any government or private sector actors whom the citizen may choose to communicate with (e.g., banks, tax authorities, and insurance companies); and
- a secure digital signature system called NemID which operates across numerous platforms, including My Page and e-Boks, and was upgraded in 2010.

Copenhagen leads the five-year strategy to make 30 of the most used electronic systems mandatory by 2015. The OECD used the Denmark e-services strategy as a case study. Denmark had a national identification number for 46 years, so it was a logical move to turn this into an e-services identifier. The first OECD report was in 2003, and Denmark became a leading test case for the work program of the Public Governance and Territorial Development Directorate within the OECD.

[147] www.borger.dk.

Four OECD reports provide a framework for analysis: *The e-Government Imperative* (2003), *e-Government for Better Government* (2005), *Rethinking e-Government Services: User-centred Approaches* (2009). Denmark was the first in a new series of country reports, *Denmark: Efficient e-Government for Smarter Public Service Delivery* (2010)[148]. Given that e-government is a driver for data sharing, this series of documents provides insight into the pressures behind data sharing, and some of the experiences of a great variety of governments in service delivery.

Denmark is a small country with 5.6 million people and a strong central government. The transparency of the web information, available for the city of Copenhagen in English, seems commendable. Copenhagen is a test site to make the currently optional e-services program mandatory, and the site exists in English, which makes it more accessible for the purposes of this report.[149]

The pages targeted at foreigners coming to Denmark are clear and straightforward, and commendably explicit about data sharing[150]:

> **Verification of personal information**
>
> Changes in the Immigration Act that came into effect on 1 August 2010 make it possible for authorities to compare information contained in various electronic registers maintained by the Immigration Service and other public authorities.
>
> The new regulation means that in all applications submitted after 1 August 2010, the Immigration Service will be able to compare information contained in its registries with records held by the Central Office of Civil Registration (CPR Office), the Buildings and Housing Registry (BBR) or in the income registry in order to ensure that applicants meet the requirements for their residence permits. Comparing information will serve as a supplement to the current control checks used to ensure that foreign nationals in Denmark continue to meet the requirements for their residence permits. Comparing information with CPR Office and BBR records will begin in autumn 2010. Such comparisons will allow authorities to ensure that a person holding a residence permit on the grounds of family reunification with a spouse is in fact living together with his/her spouse.

This is only one example, and most pages are equally explicit and clear.

Although much of the relevant information for non-residents is in Danish, this case was analyzed because Denmark is seen as a leader on e-government services and appears to manage security issues well. However, as with so many other countries, a recent high profile data breach caused concern about the program in civil society.[151]

---

[148] OECD (2010), *Denmark: Efficient e-Government for Smarter Public Service Delivery*, OECD Publishing. DOI: 10.1787/9789264087118-en.
[149] http://www.futuregov.asia/articles/2013/jan/10/copenhagen-city-e-government-change-agent/.
[150] https://www.nyidanmark.dk/en-us/coming_to_dk/verification-of-personal-information.htm
[151] Wall Street Journal May 5, 2014. *Danish Company Probed for Alleged Breach of Celebrities' Personal Data* http://online.wsj.com/articles/SB10001424052702303417104579543941470268658

Conclusions

- Denmark successfully transitioned to e-services for the citizen, and the OECD documents provide a useful analysis of structures and organizations that facilitated this, particularly the 2010 report *Denmark: Efficient e-Government for Smarter Public Service Delivery*.
- Unfortunately, there is no focus on privacy as an issue, and little information in English on the Data Protection Commissioner's website. Further research about management of privacy, particularly with respect to the citizens' portal would be useful.
- Transparency and brevity of the website information is commendable.
- The OECD country reports in the e-government series are worth further study.

VI. Citizen Expectations and Data Sharing

What are citizen expectations with respect to their data? When is data sharing acceptable and when is it objectionable? Do they coincide with the "reasonable expectations of privacy" standard assessed by the courts? If not, what should be done, if anything?

A successful information sharing project not only increases efficiency but better serves the needs and expectations of its users and its data subjects. Accordingly, expectations are a relevant and important consideration. It would not be surprising to find that, if asked, citizens would say they wanted one-stop shopping, although with some nuanced questioning other demands would likely emerge as well. One-stop shopping is only the visible tip of the data sharing iceberg, however, and it may not actually be representative of the data processing that takes place. The problem here is that detailing or mapping the extent of further data sharing is a massive problem partly because existing systems of database linkage are not well explained.

A successful information sharing project not only increases efficiency but better serves the needs and expectations of its users and its data subjects.

One example serves to illustrate this point. When the federal Office of the Privacy Commissioner audited HRSDC during 2007-08 in conjunction with the Auditor General's audit of the use of personal information, the Privacy Commissioner asked to see a list of data sharing arrangements. No such list existed, and it took several years to create a list. There appeared to be around 1,900 agreements, including arrangements with foreign governments (e.g., pension recognition), municipalities (e.g., disability benefits harmonization), and provinces (e.g., vital events, such as birth and death), as well as inter-departmental agreements.

What is the best way of keeping that list up to date, making it transparent to the citizen, and ensuring compliance with the provisions of the agreements? Including the lists of data sharing agreements each department holds under current ATIP transparency mechanisms would increase the size of the federal Infosource document significantly, and might not yield information useful to the average citizen. Is some other kind of public register required? How can one hold departments accountable for data sharing in this order of magnitude? This is the kind of chore that often falls to privacy commissioners through their audit powers, simply because no one else really wants the job

of overseeing arcane information flows. It might not be a profitable use of their time however, nor serve the greater benefit of public transparency.

Looking at other jurisdictions, note that in the U.K., the concept of "gateways" is used, performing roughly the same function as the computer connections established under Canadian data sharing agreements. The Law Commission has examined the "gateways" in its report[152], and notes particularly on page 155:

> Statutory Debris
>
> 9.26 Statutory gateways also reflect the ad hoc and contingent nature of their development where powers have not been used, are under-utilised or are sometimes simply never brought into force.

It appears that whether one uses a regulatory mechanism to achieve data sharing, or agreements/contracts between participants, it is difficult to keep them up to date.

Generally speaking, individuals, if asked, would probably expect organizations to do quite a lot of the information sharing that already happens, particularly if it results in benefits to the citizen. They expect fraud control and may not be happy if privacy and due process rights are reasons for not sharing data, at least some of the time. The reaction to the Privacy Commissioner taking the E311 case to the SCC was predictable given that Canadians freezing in January are unlikely to be sympathetic to imagined EI claimants basking in the Florida sun whilst collecting EI.

The Auditor General of Canada noted in her report on identity information[153] that information used to verify the citizen is viewed somewhat differently as personal information. Sometimes this is referred to as "tombstone data". If subject to a data breach, tombstone data can be dangerous because it may facilitate identity theft. Still, the idea that one department might update another department's data automatically may not offend citizens as much as, for instance, the health department sharing information about health conditions, with the labour department. Nevertheless, the concept of a central registry of tombstone data updated by disparate programs was a flashpoint for Australians over the Australia Card. In the current environment characterized by widespread security breaches, the same citizen objection might arise today.

Citizens have different perceptions regarding data sharing depending on their own assessment as a threat or risk and their own expectations and knowledge. The federal Privacy Commissioner commented in 2000 about the HRSDC "long file", the compilation of citizens' various work history which had been assembled in order to detect patterns in job seeking and vocation change. Two weeks after a news article reported on the OPC annual report, HRSDC received 19,000 requests from individuals for their records. People became concerned about a file rather ineptly named the "longitudinal labour force file".[154] The data matching activities using the file were not illegal, but the public was unaware of them. Eventually 70,000 people requested their records to see what the

---

[152] Law Commission, July 2014, *Data Sharing between Public Bodies A Scoping Report* http://lawcommission.justice.gov.uk/areas/data-sharing.htm.
[153] Auditor General of Canada, 2009, *Report of the Auditor General of Canada to the House of Commons, Managing Identity Information,* http://www.oag-bvg.gc.ca/internet/docs/oth_200902_e_32154.pdf.
[154] A list of interesting press references to this scandal is available at http://www.hackcanada.com/canadian/freedom/canadasbigbrother2000.html.

government knew about them that they did not know. It is clear that there is a volatile level of concern about practices involving citizen data and that the triggers for expression of concern are unpredictable. Remarkably, perhaps, the Minister rather quickly announced the dismantling of this particular data linkage. HRDC set up a data review board to ensure that all future similar research projects received senior management scrutiny.

These two examples – the "Long file" and E311 – from the same department, during the same time frame, demonstrate the varying response that the public can have to the use of their data. The meme of the "welfare cheat" is alive and well in Canada, as it appears to be in other countries. If data sharing prevents someone from unjustly claiming a benefit, particularly if that benefit comes directly from tax dollars, then public support is more likely. If on the other hand, the data matching is covert and provides information to government for unannounced purposes there is more likely to be an outcry. It is interesting, however, that in the EI example it did not seem to bother the public that the government reviewed customs cards for information for a new activity. The original purpose of the customs card is to determine what an individual or family is bringing into the country, and whether they should pay duty on the goods, not to understand what an individual is doing outside the country.

There does not appear to be any comprehensive qualitative study of Canadian reactions to intelligence sharing and risk analysis. Insurance organizations are significant users of risk modeling and careful about transparency with respect to their techniques, and they may have proprietary studies.

Given the prolonged interest since 9/11 in enhanced data collection and intelligence gathering through data mining techniques, it is likely that classified studies have been done in law enforcement, intelligence, and foreign affairs agencies about what is possible, and about public reaction. Information and privacy commissioners collectively might have an interest in requesting and examining these documents in confidence, in order to better understand the capabilities, and the direction, of developments in these areas. Given the focus of the UN on *Privacy in the Digital Age*[155], now is a good time to request access to government activities and studies.

There are a number of other potential studies that would shed light on public expectations and public response, including why people request their files from government and what they complain about. While privacy commissioners have comprehensive statistics about complaints, they are not necessarily qualitative, and the complaints may shed little light on what triggers public reactions. In some ways, one of the great mysteries of privacy is why one event, incident, or policy elicits overwhelming opposition from the public while they ignore another that may be similar or more intrusive. Interesting subjects for research include:

- Citizen responses to information sharing programs to date could include: varying degrees of concern depending on the sensitivity of information and the degree to which an individual is or may be affected (i.e., health data generally versus health data concerns held by someone who may be discriminated against on the basis of their health data; criminal records sharing generally versus concerns held by someone who has been charged with or convicted of an offence).

[155] http://www.ohchr.org/en/hrbodies/hrc/regularsessions/session27/documents/a.hrc.27.37_en.pdf

- Examination of the continuum between privacy and convenience: When does an individual start to feel that risks outweigh convenience? How stable is the continuum? How do security breaches and identity theft concerns affect the perception? What about changes in government, or control (foreign ownership) of a company?
- Mapping the level of effort required to understand what is happening to the data of the individual.
- Group privacy: Who has the responsibility to ensure that information about one individual does not have implications for the profile or privacy of another individual or group with whom there is a familial, ethnic, geographic, or other link?

Case studies in this report demonstrate the lack of understanding that citizens bring to the modern Information Society. Volatile reaction to some personal data activities brought down many government initiatives (e.g. Australia Card, joined-up justice or public key infrastructure initiatives). A better sense of public expectations would allow stakeholders to find better and more acceptable balances between interests that compete with privacy.

VII. Examining Risk in Data Sharing Projects and Proposals

It is customary now in Canada to think about the use of PIAs and security threat risk assessments (TRAs) when evaluating the risk of projects involving personal data, although this is not the case in all other jurisdictions.[156] To be effective, these tools must be applied appropriately in practice, and not become simply procedural. They must become part of a management framework, not a tick-off box. They have to be scoped appropriately, and a frequent criticism is that a PIA is too narrow and misses issues or risks which impact implementation. A few examples illustrate this point.

If the mitigation for internal abuse of a data system is the maintenance of audit logs, the mere existence of audit logs is insufficient to give confidence that those who have access to the system will be deterred from abusing it. True mitigation requires that the following questions be addressed:

- What does the audit log track? How detailed is the data (e.g., date stamps, time stamps, access control number, IP address, etc.)? Does the audit log include the purpose of an access? Are the audit logs immutable?
- Who reads the audit logs, and how long are they kept?
- Who is responsible for oversight of user access? Is there a separation of responsibility between those who supervise administration of the system, or security of the system, and those who verify the audit logs (e.g., does the auditor in the organization have a role, or is it the security department?)

---

[156] The Treasury Board of Canada replaced the original privacy impact assessment policy, dated 2002, but materials are available here: http://www.tbs-sct.gc.ca/pol/doc-eng.aspx?id=18308&section=text. The Alberta PIA Guide for the Health sector is here http://www.oipc.ab.ca/Content_Files/Files/PIAs/PIA_Requirements_2010.pdf,. Many other examples are available online.

- Is the system responsive or passive? For instance, is it possible to put a monitor on particular individuals (e.g., in a hospital setting, if a celebrity is admitted as a patient, etc.)? Will access produce an immediate response and not just a log entry for review months later?
- Will those found to abuse access privileges be sanctioned in a meaningful (and visible) way?

Sometimes in PIAs, questions regarding process issues, such as how audit logs are administered, are rebuffed as out of the scope of a PIA. Yet when the efficacy of the control impacts privacy, it seems that it should not be out of scope.

Another example relates to the funding of initiatives. Supporters of data sharing activities often claim that sharing will be more efficient and will result in cost savings. Estimates of savings may be exaggerated or may not be realized at all. If promised savings included in budgeting do not occur, shortfalls will result. It is advisable to investigate exactly which budget privacy risk mitigations are to come from, in order to ensure that money can still be found in the budget for privacy mitigations, if the potential savings fail to materialize. Once again, detailed budget allocations, and program review to determine savings are often deemed out of scope. This approach fails to recognize that the success of a program can depend on whether funds are available to administer the mitigations.

With data sharing, policy clashes between privacy and cost savings are common. A data sharing activity justified by cost savings should have a sunset so that an audit can determine if actual savings resulted. The sunset should force a reauthorization of the data sharing program, and the audit will provide the necessary factual information. This is important because programs tend to have a life of their own after a period, whether or not the justification for the programs remains.

With data sharing, policy clashes between privacy and cost savings are common.

In any risk analysis of data sharing projects, privacy practitioners should insist on broad, multi-faceted examination of risks and benefits to the extent possible, not merely a narrowly scoped examination of legal privacy risks or potential breaches. An entire system needs to be examined to ensure that it can support an appropriate approach to the protection of personal information as part of the overall management framework. This is sometimes referred to as a "holistic assessment".

In some areas of this risk assessment, information and privacy commissioners may have no formal authority or role, but this should not be a deterrent to raising the right questions at the right time. In a classic risk assessment, the likelihood of the risk is assessed against the severity of the impact if it does occur, leading to a classification of risk as low, medium, or high. Privacy commissioners who deal with complaints are in a position to provide expert advice in this assessment. Another key element in a proper risk assessment is naming the party responsible to monitor that risk, making sure that the assessment of likelihood was accurate, and determining that mitigations for the risk are actually put in place or ready. It is also important to check back to make sure that the mitigations are working, and if not, to come up with new ones. A privacy commission may be able to carry out some or all of these oversight tasks.

Based on the analysis of the various data sharing initiatives and strategies outlined in section IV, the key risks and mitigations have been identified, and are clustered around the following themes.

Legal Authority

- Organizations require the legal authority to collect, use and disclose or share the data.
- Separate organizations require contractual authority, sharing agreements, or, in the case of separate nations, a treaty or other authority to share data.
- All authority relied upon for data sharing, including contracts with the private sector, must be reviewed for constitutional correctness and legal compliance.
- Personal data should be maintained in a way that maximizes the application and enforceability of privacy law.
- Independent oversight of all authorities is essential.

Potential mitigations:

- New regulations or new legislation
- Regulatory impact assessment
- Charters of data sharing partners
- Contracts for major activities reviewed by data commissioners
- Public and civil society comment during planning, contracting, and implementation stages of data sharing

Procedural Fairness

- This study suggests why it is insufficient for a project to be compliant with the legal framework. Public acceptance depends on many factors, with legal and constitutional compliance being only some of them. More generally, a project must be seen as fair to the citizen in order to be accepted.
- Assessment of constitutional risk is one tool that is sometimes used to assess fairness, but too often that assessment results in a review of case law rather than a thoughtful exploration of whether the proposal meets "the smell test". Some activities are deemed to be too "creepy" to be acceptable.
- Fairness often requires a political and ethical judgment – those are two different types of judgments – and not just a legal one.
- Where individual interests are directly at risk, formal due process procedures are essential.

Potential mitigations:

- Focus groups of affected citizens may raise issues that could lead to fruitful discussions of procedural fairness, ethics, and "the smell test", participation by privacy commissioners could help ensure that the process is unbiased.
- Participation of constitutional scholars and civil society on working groups is more likely to lead to better analysis.
- An internal ombudsman or privacy officer for a data sharing initiative, in addition to privacy commissioners, could be useful to monitor due process and fairness issues, and to receive internal complaints, receive whistleblowers, etc.
- Information materials about fundamental rights need to be available.

Financial Risk

- The existing record of failed government IT projects suggest strongly that major hardware or software projects present a substantial risk that many will never reach implementation. No one ever thinks that their project will fail, but history demonstrates otherwise.
- Inadequate funding, whether from optimistic vendor estimates, optimistic projected program savings, or optimistic timelines for completion are significant risks in government IT projects.
- Cutbacks in spending can impact ongoing projects, and make risk mitigations inoperative (e.g., staff cuts preventing audit log review, separation of duties, etc.). The possibility exists for the worst of both worlds; insufficient funding to achieve the goals of the data sharing while privacy protections disappear because of funding shortfalls.

Potential mitigations:

- Funding estimates for projects should be subject to public consultation as well as independent second opinions from appropriate experts.
- Program managers must constantly determine that privacy risk mitigations are still in place and not dropped. Regular reporting to privacy commissioners during development and initial implementation may be valuable.
- Funding for privacy mitigations might be provided as a percentage of overall spending so that the privacy funding cannot disappear altogether. The possibility that some project funding should be provided to privacy commissioners to conduct oversight should be considered. The funding would have to be allocated in an advanced, fixed, and independent way.

Organizational Commitment to Privacy

Ross Anderson expressed the bureaucratic fear of mishandling privacy in *Database State*:

> There is a sense in the senior civil service and among politicians that the personal data issue is now career-threatening and toxic. No-one who values their career wants to get involved with it. This is irresponsible and short-sighted. Like Chernobyl, the database state has been a disaster waiting to happen. When it goes wrong, some brave souls need to go in and sort it out while others plan better ways to manage things in the longer term.[157]

This speaks to a broad problem related to organizational commitment: Who owns the privacy problem? In a mature organization that realizes privacy is fundamental to the service they give the citizen, the organization is accountable and takes responsibility for ensuring that the organization has a mature privacy program, including competent senior officers in charge of it, training, PIA review, audit, etc. Others may regard privacy and procedures as something done to ensure a privacy

This speaks to a broad problem related to organizational commitment: Who owns the privacy problem?

[157] *Database State,* http://www.jrrt.org.uk/sites/jrrt.org.uk/files/documents/database-state.pdf at p.9.

commissioner does not question activities. In these situations, privacy is not regarded as part of the organizational goal. Obviously this is directly related to senior management leadership, and the problem Anderson describes above may apply.

If privacy as a policy issue has become a risk, it will become difficult to get the focus on some of the intractable problems:

- New technologies such as data mining and cloud services raise complex privacy risks, requiring significant expertise and analytical skills, not to mention dedication to sound public policy. Staff with the knowledge and experience may not be available in the government. Contractors may have a conflict of interest if they are working for companies who are selling those products.
- It was often said in the past that concern for privacy was "a mile wide and an inch deep". Given the increased focus and attention to privacy, that old view may no longer have any validity. Public concern about privacy is sometimes both wide and deep, but it is often unpredictable. A lack of commitment allows organizations to make gestures to privacy, and focus on other political and policy issues that are also important to Canadians. Absent a trigger to put the right focus on privacy – such as negative press attention, a politically astute Minister or senior staff, or a well-timed nudge from a privacy commissioner – an organization may fail to make necessary or even adequate adjustments for privacy in a timely manner.

Potential mitigations:

- Leadership is necessary to achieve organizational commitment. Senior politicians and public servants need to be engaged in the issues, which may require lobbying, engagement through participation in conferences and debates, or parliamentary focus.
- A privacy commissioner can sometimes have an outsized influence by nudging senior officials in the right way and at the right time. There is no manual for exerting influence in informal ways.
- Ownership of privacy as an issue has to reach the middle ranks of an organization in order for the culture to change. As an example, the committee responsible for reviewing data research at HRSDC, after the debacle of the "long file", took their jobs seriously and took ownership of privacy as an important part of the culture.
- Media attention to privacy issues may raise the status or ranking of privacy in the organization.
- Public interest groups can play a vital role in holding agencies and politicians accountable over privacy, with a privacy commissioner helping to keep the process honest and neutral.
- If and when a privacy equivalent of Chernobyl occurs, a plan to positively influence actors involved by solving the problems and enabling them to take pride in their work will help. If, on the other hand, public servants are scapegoated after a breach or policy mistake, the "scalded cat" syndrome is apt to take over (i.e., everyone runs away and hides). One neglected task in privacy risk management is a thoughtful crisis intervention plan that helps organizations respond positively about privacy at times of disaster.
- As the U.K. children's services example shows, horror stories can cut both ways. A dramatic story can promote other concerns and override privacy protections. When privacy is on the political or emotional defensive, a privacy commissioner can step

forward and offer suitable balancing comments during periods of intense pressure. This can be a difficult role, but a necessary one.

Security Management

- Security protocols and procedures using generally accepted standards and best practices need to become requirements in the contracts and charters of all projects. Reinventing the security wheel should be necessary only in rare cases. The IRS example shows that published security standards and protocols can make requirements clear to all data users. Using well-recognized standards should achieve both lower costs and better security than any ad hoc approach.
- Regular reporting on security audits should be included in project management plans.
- Audit logs for data use and disclosure provide critical checks. They need to be funded properly and actually used for oversight.
- Training is essential for all staff involved in the project. This is not a one-time event; it must be repeated as required.
- Sanctions for staff who do not follow security procedures need to be significant, administered fairly, and visible as appropriate. This requires regular checking.

Potential mitigations:

- External audit of security measures, procedures and protocols, including management of audit logs, may be more reliable than internal self-discipline, although both are helpful. The IRS example shows how an agency that shares data and bears much of the institutional and political risk of data sharing can conduct audits of those who receive the data.
- Data analytics of audit logs can be extremely useful, and software that is being purchased for risk analysis of clients might be useful for audit logs.
- Whistleblowing should be encouraged. An independent ombudsman attached to the project or one that exists for other purposes could investigate reported problems.
- A privacy commissioner cannot take responsibility for all security oversight but can assist through the preparation of checklists for proper high-level processes and procedures and use of acceptable government or private sector security standards.

Project Scope Creep

One of the problems with modern predictive data analytics capability is the atmosphere that it sets up within an organization. Once data elements have been shown to accurately predict risk, the next question is, what else can be predicted? This creativity may be useful, but it potentially clashes with privacy as a value, with existing legislative goals of anti-discrimination, and with respect for the dignity of the individual humans involved. This is of course not a new problem; data matching had a similar attractive quality. As in the E311 example, once dates of departure and arrival dates are used to calculate the time out of the country for EI eligibility, what other uses could this data element serve? Immediately one thinks of health insurance eligibility since Canadian snowbirds going south for the winter might exceed the six months they are allowed out of the country before their health insurance lapses. Would provinces like to be alerted by CBSA when someone's E311 card signals they overstayed outside the country and are temporarily ineligible for health insurance? Pension eligibility is another issue, particularly for immigrants who must have 10 years of continuous residence in Canada before they are eligible for the Old Age Security pension.

Similarly, data elements collected may expand, particularly where reporting becomes mandatory or simply because it is easy to do. In the U.K. children's services case, a particular tragedy instigated more data tracking. What teacher would not document a file with bruises noted on a child if failure to do so could lead to allegations of neglect in the event of abuse? Once it becomes routine to note "schoolyard bullying" on some children's files, how difficult would it be to distinguish between the usual schoolyard roughness, and particular cases of harassment? Better to err on the side of caution and report; soon the data becomes massive. This is certainly a risk in financial crimes reporting, where failure to report "suspicious activity" may carry criminal penalties.

Guarding against scope creep can be difficult, but identifying the key risks will help:

- Once a new use of data is found, there is a risk that further thinking about the usefulness of that data element will lead to new uses and more data sharing.
- Once a data element is found to be useful, further information (i.e., new data elements) may be desired.
- Costs of running data analytics programs or data warehouses tend to favour scope creep as high volumes of data and repeat use of software are needed to justify costs.
- Once barriers to sharing with one agency or partner are dropped, there is a risk that the organization will not be able to refuse sharing with another agency. In the E311 example, use of the data was permissible to enforce the laws of Canada, which is broad enough to cover numerous other laws and departments. If the Charter's expectation of privacy is ignored or unfairly assessed, what is the effective block to wholesale sharing?

Potential mitigations:

- Data sharing and extended data collection may be legal, or governments may be able to easily pass legislation or regulations that make them legal. However, the impact of public opinion needs to be examined. A full privacy risk assessment does not simply look at legal risk.
- Tax authorities have considerable authority to collect and share data. They guard that legislated authority jealously though, for fear that sloppiness on the part of their partners in data sharing may bring about disrepute, which could impact their legislated ability to acquire data. In this respect, the partners in a data sharing arrangement should be assessed in terms of their "skin in the game". Those with the most to lose will likely be the best partners in data protection and procedural fairness.
- In many cases, more data means more responsibility. More data may mean learning more than budgets permit an agency to mitigate or investigate. Right-sizing data collection to recognize bureaucratic and budget limits may minimize privacy risks and the costs and consequences of security breaches.
- A privacy commissioner can play a public role in identifying and raising questions about new data sharing activities. A published list of standards that should be met before data sharing activities expand might be more helpful and would avoid ad hoc responses. A reminder by the commissioner about the bureaucratic risks of too much data collection may be effective.

Data Mining and Data Elements

Numerous risks are associated with data mining:

- Data mining is the latest bright shiny toy. It is not clear that it is always useful in the government services context, but IT departments want to buy it because it is state of the art. Following 9/11, American law enforcement and intelligence agencies purchased new data services from eager vendors, but results were not always what they expected.[158]
- Predictive analytics may be useful for marketing and determination of disease vectors, it is less so in social services and every other sector of public service where individuals are entitled to service without discrimination. In fact, the White House report on Big Data suggests that discrimination may be an unwanted consequence of using of data analytics.
- Big data as a concept is directly contrary to the fundamentals of privacy, namely scope and volume limitation.
- There is a significant risk that inaccurate data will lead to discrimination and inaccurate predictions. The same risk exists even when data is accurate but the analytics are misguided. Data accurate enough for one purpose, in one databank, may not be accurate in a different context or setting. Many data elements, such as name, address, and even sex, are not that simple, and different activities need different levels of information. For instance, marital status data for one program may simply depend on whether there is/was a spouse/partner, for another program the criterion could be that the partner currently resides with the individual, for another program the criterion could be a marriage certificate. A simple data element may not reveal the information needed to make a decision.
- There is a risk that people will either exaggerate how different data mining or big data is, in order to reject privacy as a concept, or underestimate the key differences - "It's all new!" or "It's the same as it always was!". Data protection law and principles do not lose their relevance because of new technology or new applications.
- U.S. companies may be leaders in data analytics capability (e.g., IBM, SAS), and data collection companies (e.g., Axciom, Trans Union, Google, Choicepoint, Facebook) but some may be laggards in data protection and human rights. The U.S. is currently leading the discourse on big data.

Potential mitigations:

- Comprehensive regulatory impact assessments are necessary if predictive analytics are going to be used with an added focus on Charter rights
- Cost-benefit analysis should be done, based on facts relevant to the study in question, not extrapolated from unrelated exercises.
- Data elements need to be assessed for relevance and accuracy.
- Sunset provisions are essential for evaluating whether a program is truly successful and cost-effective.
- In this arena, privacy commissioners may be able to focus collectively on this issue. The exaggerated claims of new tools need careful examination and balanced assessments.

---

[158] See generally, Robert O'Harrow, Jr., No Place to Hide (2005).

Transborder Legal Demands and Jurisdiction

- The availability of data for use in foreign courts is currently under litigation in several jurisdictions. There is no certainty as to whether individuals can enforce their rights when the data is held outside the country.
- When data is held outside the country, there is no certainty that data subjects will be notified when there is a data breach, which puts them at risk of identity theft among other harms.
- Certain kinds of profiling that are safe in some countries may put a citizen (or dual citizen) at risk when travelling outside the country. (e.g., LGBT, political activism, or membership in certain religious groups). This makes it imperative that organizations be aware of the potential impacts of data aggregation, and the harms it can cause through the creation of profiles that may not be apparent from their own datasets. Since organizations may think the data they are sharing appears innocuous if they do not recognize indicators, this risk may go undetected. See next section on group privacy.

Potential mitigations:

- The guidance prepared by the federal TBS for contracting in the federal government is useful.[159]
- Data commissioners may wish to require that data remain in a jurisdiction where there is no question regarding their ability to enforce data protection law.
- A privacy commissioner may wish to work with legal authorities to identify privacy concerns from foreign legal demands and to develop appropriate responses. A privacy commissioner may also choose to inform government agencies and locally based companies about the risks of storing personal information in foreign jurisdictions, whether done directly or through the purchase of services from vendors who operate in whole or in part in foreign jurisdictions. If there are outsourcing rules applicable, the rules need to be complied with.

Group Privacy

Group privacy is currently not well understood in data protection nor is there much research on the topic of how best to protect it under existing law. Human rights law may have relevance in this context:

- Some groups may experience invasion of privacy or discrimination to a greater extent in data sharing activities, depending on the situation.
- Some groups may be more resistant to data disclosure or data use because of their history, religion, or perception of invasion of group privacy.
- Data mining algorithms may casually create groups or profiles that may have persistence (e.g., potential young offenders, potential diabetic patients, potential mothers of underweight children, etc.) and that may stigmatize group members in major ways.

---

[159] http://www.tbs-sct.gc.ca/atip-aiprp/tpa-pcp/tpa-pcp01-eng.asp.

Potential mitigations:

- Data analytics programs should be analyzed through targeted PIAs that examine any groups created, particularly in the case of predictive analytics.
- Certain groups that can be easily identified should be consulted to see if they are interested in having their own ombudsman or advocate to supervise or audit large systems (e.g., neighbourhood groups, indigenous peoples, disabled, etc.). An oversight board of various representatives might be one way to achieve this in a fair and unbiased way.
- More awareness of group privacy concerns is needed at all levels, even within the privacy advocacy community.

Research Ethics

Identifiable personal data used for statistical analysis when "joined-up government" should be subject to research ethics review. There are a number of risks:

- Data, even when anonymized, can be linked with other data collections and re-identified.
- Research findings are often public, depending on the stipulations that pertain to funding.
- Researchers may be unaware of the sensitivity of certain data and conclusions about individuals or groups

Potential mitigations:

- The organization holding the data could set up a research review board, and insist on specific PIAs or research ethics reviews prior to allowing access to the data
- Some research protocols could be sent to the relevant data commissioners for review.
- Concerns about re-identification and misuse of data made available for research can be controlled through data use agreements that bind data recipients and hold them accountable.[160]

Public Relations and Communications

Communications concerning data sharing obviously contains a number of risks as is evident from the case studies considered in this report, but so does not communicating. Communicating risk itself is one of the most complex and difficult tasks of risk management, as the mere knowledge of a risk brings with it potential liability (i.e., if you knew about the risk, why did you not do anything about it?). Plausible deniability is often recommended with the best of intentions in both industry and government. Senior management may choose not to be briefed on risks.

---

[160] See Robert Gellman, The Deidentification Dilemma: A Legislative and Contractual Proposal, 21 Fordham Intellectual Property, Media & Entertainment Law Journal 33 (2010), http://ir.lawnet.fordham.edu/cgi/viewcontent.cgi?article=1277&context=iplj.

The following is a list of some risks inherent in communications, but this is a big topic and the list is not exhaustive.

- There is a risk that insufficient communications and transparency about the data sharing project will create suspicion in various stakeholder groups.
- There is a risk that open discussion of privacy risks will trigger a negative reaction that threatens the initiative.
- There is a risk that insufficient awareness of technology capability, data management practices, and current data holdings, will precipitate an over-reaction to a modest and perfectly legal data sharing practice.
- There is a risk that individuals' expectations with respect to the protection of their personal data could be raised to unsupportable levels.
- There is a risk that any potential communications will be regarded negatively by organizations engaged in data sharing if they do not wish to be transparent or they wish to tightly control messaging.
- There is a risk of losing control of messaging, which has increased substantially with the advent of social media.

Potential mitigations:

- The benefits of transparency, with descriptions and examples from other jurisdictions and projects, could be publicized. The authors note that the U.K. government is using social media to be transparent about their data sharing plans in 2013-14, which is a more open approach than previously done.
- Stakeholder meetings, including as broad a range as possible of academia, NGOs, other government organizations, and outside experts, can mitigate many communications risks and deficits, and reports of the meetings can provide neutral information for citizens. Meetings can now easily be publicly accessible, both for visibility and participation, via the Internet.
- Town hall type meetings can bring out citizens to participate in discussion, and local groups can continue discussion after the main sessions.

The elements described above are broad categories. For each one there could be a more complete breakdown of risk elements and mitigations, but this suffices to give a background for discussion of strategies and approaches to evaluating, commenting on, and intervening effectively on data sharing initiatives.

VIII. Conclusions

There is no one course to chart with respect to data sharing. This report has attempted to sketch out where the issues are the same as they have always been since the first data collections on computers, and where they are different because of powerful new technologies. Similarly, some risks are about the same, and others have increased significantly. Trust in governments has always been somewhat fragile – with or without technology – but the risks of identity theft, social exclusion, and reputational damage may well have gone up because of today's big data. Because some risks have increased significantly, it is important that remedial action takes place. Fortunately, those risks are

owned by many stakeholders, so that information commissioners can play a broker role in raising awareness, issuing advice, promoting higher standards, and persuading all stakeholders to take privacy and the respect for the dignity and autonomy of each individual seriously.

All Canadians want the benefits of electronic government services, and reduction of administrative burdens. Some of us still want our privacy and autonomy too. We should go into discussions of data sharing fully informed of the risks and possible strategies to mitigate those risks. The authors hope that this report makes a useful contribution to that vital discourse.

References

6, Perri, "Joined-Up Government in the Western World in Comparative Perspective: A Preliminary Literature Review and Exploration", Journal of Public Administration Research and Theory: J-PART Oxford, United Kingdom: Oxford University Press 14: pp.103–138.

ABC News, "Google Taking Requests to Censor Results in Europe". (30 May 2014), http://news-headlines.info/2014/05/30/google-taking-requests-to-censor-results-in-europe-abc-news/.

Albanesius, Chloe, "The NSA's Prism: What They're Saying" (7 June 2013) http://www.pcmag.com/article2/0,2817,2420128,00.asp.

Alberta, Office of the Information and Privacy Commissioner, Alberta PIA Guide for the Health Sector, http://www.oipc.ab.ca/Content_Files/Files/PIAs/PIA_Requirements_2010.pdf.

Amberhawk Training, Push For New Data Sharing Powers As Law Commission's Data Sharing Report is Shelved (9 Oct. 2014), http://amberhawk.typepad.com/amberhawk/2014/10/push-for-new-data-sharing-powers-law-commissions-data-sharing-report-is-shelved.html.

Anderson, Ross, Brown, Ian, Dowty, Terry, Inglesant, Philip, Heath, William, & Sasse, Angela, Database State: A Report Commissioned by the Joseph Rowntree Reform Trust, Joseph Rowntree Reform Trust, York UK, 2009, http://www.jrrt.org.uk/publications/database-state-full-report.

APEC Privacy Framework (2005), www.apec.org/Groups/Committee-on-Trade-and-Investment/~/media/Files/Groups/ECSG/05_ecsg_privacyframewk.ashx.

Auditor General of Canada, Public Service Management Reform: Progress, Setbacks and Challenges (2001), http://www.oag-bvg.gc.ca/internet/english/meth_gde_e_10222.html.

Auditor General of Canada, Report of the Auditor General of Canada to the House of Commons, Managing Identity Information (2009), http://www.oag-bvg.gc.ca/internet/docs/oth_200902_e_32154.pdf.

Australia, Department of the Prime Minister and Cabinet, "Ahead of the Game: Blueprint for the Reform of Australian Government Administration Overview" (Feb 2011), http://www.dpmc.gov.au/reformgovernment/.

Australia, Finance Department, Gershon, Peter, "Review of the Australian Government's Use of Information and Communication Technology" (2008), http://www.finance.gov.au/publications/ICT-Review/.

Australia, *Human Services (Centrelink) Act 1997*: Act No. 31 of 1997 as amended, http://www.austlii.edu.au/au/legis/cth/consol_act/hsa1997266/.

Australia, Human Services: Bilateral Head Agreement between Secretary of Department of Human Services and the Secretary of Department of Health and Aging: 2012-2015, http://www.humanservices.gov.au/spw/corporate/about-us/resources/bilateral-head-agreement.pdf.

Australia, *Human Services Legislation Amendment Act 2011: An Act to amend the Medicare Australia Act 1973, the Commonwealth Services Delivery Agency Act 1997 and the Child Support (Registration and Collection) Act 1988, and for other purposes.* http://www.comlaw.gov.au/Details/C2011A00032.

Australia Privacy Foundation: http://www.privacy.org.au/Papers/.

BC Civil Liberties Association, Privacy Groups Demand Halt to BC ID card rollout. 8 Feb 2013. http://bccla.org/news/2013/02/privacy-groups-demand-halt-to-bc-id-card-roll-out/.

BC b-sides Blog: Brooke: BC Services Card Consultation (22 April 2014), http://www.bcbsides.ca/bc-services-card-consultation/.

B.(R.) v. Children's Aid Society of Metropolitan Toronto [1995] 1 S.C.R. 315, http://www.canlii.org/en/ca/scc/doc/1995/1995canlii115/1995canlii115.html.

Barr, Alistair & Winkler, R., "Google Offers Right to be Forgotten Form in Europe" (30 May 2014), Wall St. Journal. http://online.wsj.com/articles/google-committee-of-experts-to-deal-with-right-to-be-forgotten-1401426748.

Blencoe v. British Columbia (Human Rights Commission), 2000 SCC 44 (CanLII), [2000] 2 S.C.R. 307.

Bomsdorf, Clemons, "Danish Company Probed for Alleged Breach of Celebrities' Personal Data" (5 May 2014), Wall Street Journal. http://online.wsj.com/articles/SB10001424052702303417104579543941470268658.

British Columbia Government, Photo BC Services Card: See the Card, http://www2.gov.bc.ca/gov/topic.page?id=C71B580C55204AAC98B35C6B75D8860D&title=Photo%20BC%20Services%20Card.

British Columbia Government, BC Services Card: Use the Card, http://www2.gov.bc.ca/gov/topic.page?id=1AEB073331D547448009E506D6DAC395&title=Use%20the%20Card.

British Columbia Government, Digital Services Consultation, http://www2.gov.bc.ca/govtogetherbc/consultations/digital_services.page, http://engage.gov.bc.ca/digitalservices/consultation-results/.

British Columbia, Digital Services Consultation, Fall 2013: Minister's Response (2013) http://www.gov.bc.ca/citz/down/DigitalServicesConsultation_report_web.pdf.

British Columbia, Ministry of Technology, Innovation and Citizen's Services, Provincial Identity Information Management Program: BC Services Card, http://www.cio.gov.bc.ca/cio/idim/bcservicescard.page.

British Columbia, Office of the Information and Privacy Commissioner, Privacy and the USA Patriot Act: Implications for British Columbia Public Sector Outsourcing (2004), https://www.oipc.bc.ca/special-reports/1271.

British Columbia, Office of the Information and Privacy Commissioner, BC Services Card: Phase 1 Review (5 Feb 2013), https://www.oipc.bc.ca/news-releases/1502.

Cabinet Office (UK) data sharing paper (dated 28th July 2014), available on google docs at

https://docs.google.com/document/d/1g6kpiRUpgECnR2IXCuP0O1_VmuMMBgbD-oCmQI4wHVE/edit?pli=1.

Canada, Canada Borders Services Agency, Policy on the Disclosure of Customs Information: Section 107 of the *Customs Act*, http://www.cbsa-asfc.gc.ca/agency-agence/reports-rapports/cd-da/pdci-pdrd-eng.html.

Canada, *Canadian Charter of Rights and Freedoms*; The Constitution Act, 1982, Schedule B to the Canada Act 1982 (UK), 1982, c 11, http://canlii.ca/t/ldsx.

Canada, *Customs Act* (R.S.C., 1985, c. 1 (2nd Supp.), http://laws-lois.justice.gc.ca/eng/acts/C-52.6/.

Canada, *Employment Insurance Act* (S.C. 1996, c. 23), http://laws-lois.justice.gc.ca/eng/acts/E-5.6/index.html.

Canada, Financial Transactions and Reports Analysis Centre of Canada (FINTRAC), http://www.fintrac.gc.ca/.

Canada, Information Canada, *Privacy and computers: a report of a Task Force established jointly by Department of Communications/Department of Justice* (1972), Ottawa: Information Canada.

Canada, Office of the Auditor General. Public Service Management Reform: Progress, Setbacks and Challenges (2001), http://www.oag-bvg.gc.ca/internet/english/meth_gde_e_10222.html.

Canada, Office of the Privacy Commissioner of Canada, "Privacy Concerns with FINTRAC Remain Following 2 Separate Audits" (24 October 2013), https://www.priv.gc.ca/media/nr-c/2013/nr-c_131024_e.asp.

Canada, Office of the Privacy Commissioner of Canada, 1996/97 Annual Report, https://www.priv.gc.ca/information/ar/02_04_05_e.asp#014.

Canada, Office of the Privacy Commissioner of Canada, 1995/96 Annual Report, https://www.priv.gc.ca/information/ar/02_04_05_e.asp#014 =.

Canada, Office of the Privacy Commissioner of Canada, Audit Report of the Office of the Privacy Commissioner of Canada: Financial Transactions and Reports Analysis Centre of Canada: Final Report (2013), https://www.priv.gc.ca/information/pub/ar-vr/ar-vr_fintrac_2013_e.pdf.

Canada, Office of the Privacy Commissioner of Canada, Audits of Major National Security Programs Raise Concerns for Privacy, (17 November 2009), https://www.priv.gc.ca/media/nr-c/2009/nr-c_091117_e.asp.

Canada, Office of the Privacy Commissioner of Canada, The Challenges Posed to Privacy by Technology, Julien Delisle speech to Chamber of Commerce of Thérèse-de-Blainville (28 Jan 1998), https://www.priv.gc.ca/media/sp-d/archive/02_05_a_980128_e.asp.

Canada, Office of the Privacy Commissioner of Canada, An Overview of Canada's New Private Sector Privacy Law – the Personal Information Protection and Electronic Documents, (speech by Jennifer Stoddart 2004), https://www.priv.gc.ca/media/sp-d/2004/vs/vs_sp-d_040331_e.asp.

Canada, Privy Council Office, What We've Heard: Blueprint 2020 Summary Interim Progress Report, Blueprint 2020: A Vision for Streamlining Canada's Public Service http://www.clerk.gc.ca/eng/feature.asp?pageId=361.

Canada: Shared Services Canada, Cloud Computing: Outstanding Challenges Architecture Framework Advisory Committee (16 July 2013), http://itac.ca/wp-content/uploads/2013/07/AFAC_Cloud-Computing_-Challenges-_July-2013.pdf.

Canada: Shared Services Canada, Why Shared Services Canada? (13 September 2013), http://www.ssc-spc.gc.ca/pages/bckgrnd-cntxt-eng.html.

Canada, Treasury Board Secretariat, Federating Identity Management in the Government of Canada: A Backgrounder (2009), http://www.tbs-sct.gc.ca/sim-gsi/docs/2011/fimgc-fgigc/fimgc-fgigc01-eng.asp.

Canada, Treasury Board Secretariat, Guidance Document: Taking Privacy Into Account Before Making Contracting Decisions, http://www.tbs-sct.gc.ca/atip-aiprp/tpa-pcp/tpa-pcp01-eng.asp.

Canada, Treasury Board Secretariat, Privacy Impact Assessments, NOTE: The Treasury Board of Canada has replaced the original privacy impact assessment policy, dated 2002, but materials are available here: http://www.tbs-sct.gc.ca/pol/doceng.aspx?id=18308&section=text.

Canada's Big Brother (blog), http://www.hackcanada.com/canadian/freedom/canadasbigbrother2000.html.

Canada Employment Insurance Commission: http://www.esdc.gc.ca/en/ei/commission.page.

Canadian Press "Powerful New Card to Replace B.C. Care Card" (Jan 8 2013), http://www.cbc.ca/news/canada/british-columbia/powerful-new-card-to-replace-b-c-care-card-1.1354302.

Century 21 Canada Limited Partnership v. Rogers Communications Inc., 2011 BCSC 1196 (CanLII), http://canlii.ca/t/fn00h.

Cheskes v. Ontario (Attorney General), 2007 CanLII 38387 (ON S.C.). http://www.canlii.org/en/on/onsc/doc/2007/2007canlii38387/2007canlii38387.html.

Clarke, Roger, "The Realities of Bowen's Service Delivery Reform" (17 Dec 2009), http://www.rogerclarke.com/DV/SDR-0912.html.

Clarke, Roger, "Centrelink Smart Card Technical Issues Starter Kit" (1998), http://www.rogerclarke.com/DV/SCTISK.html.

Cloud Computing: Outstanding Challenges: Architecture Framework Advisory Committee (16 July 2013), http://itac.ca/wp-content/uploads/2013/07/AFAC_Cloud-Computing_-Challenges-_July-2013.pdf.

Computer Matching and Privacy Protection Act of 1988: Public Law 100-503, 102 Stat. 2507, gpo.gov/fdsys/pkg/STATUTE-102/pdf/STATUTE-102-Pg2507.pdf.

Computer Weekly, "Inland Revenue and EDS: Divorce Impossible?" (October 2002), http://www.computerweekly.com/feature/Inland-Revenue-EDS-Divorce-Impossible.

Customs Act (R.S.C., 1985, c. 1 (2nd Supp.), http://laws-lois.justice.gc.ca/eng/acts/C-52.6/.

Data Sharing Blog, Updates from civil society engagement with the UK Government on data sharing http://datasharing.org.uk/whos-involved/.

Denmark, Danish Immigration Service, Verification of Personal Information (8 April 2010), https://www.nyidanmark.dk/en-us/coming_to_dk/verification-of-personal-information.htm.

Dixon, P. & Gellman, R., The Scoring of America: How secret consumer scores threaten your privacy and your future (2014), San Diego, CA: World Privacy Forum. http://www.worldprivacyforum.org/category/report-the-scoring-of-america/.

EuroNews, "Google Offers Right to be Forgotten Form to Remove Personal Data" (31 May 2014), http://www.euronews.com/2014/05/31/google-offers-right-to-be-forgotten-form-to-remove-personal-data/.

European Commission, Factsheet on the Right To Be Forgotten Ruling, http://ec.europa.eu/justice/data-protection/files/factsheets/factsheet_data_protection_en.pdf.

European Commission, Safeguarding Privacy in a Connected World

A European Data Protection Framework for the 21st Century, http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52012DC0009&from=en.

European Union, Article 29 Working Party, Opinion 01/2014 on the application of necessity and proportionality concepts and data protection within the law enforcement sector (27 February 2014), http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp211_en.pdf.

European Union, Article 29 Working Party, Statement of the WP29 on the impact of the development of big data on the protection of individuals with regard to the processing of their personal data in the EU (Adopted 16 September 2014), http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp221_en.pdf.

FAME, Framework for Multi-Agency Environments, http://www.fame-uk.org/.

European Union, *Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data*, http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:en:HTML.

Foundation for Information Policy Research, "Children's Databases: Safety and Privacy" (2007) http://www.cl.cam.ac.uk/~rja14/Papers/kids.pdf.

Gellman, Robert, "The De-identification Dilemma: A Legislative and Contractual Proposal", 21 Fordham Intellectual Property, Media & Entertainment Law Journal 33 (2010), http://www.bobgellman.com/rg-docs/RG-Fordham-ID-10.pdf.

Gellman, Robert, "Fair Information Practices: A Basic History" (2014), http://ssrn.com/abstract=2415020.

Glaxo Wellcome PLC v. M.N.R., [1998] 4 FC 439, 1998 CanLII 9071 (FCA), http://canlii.ca/t/4mff.

Godbout v. Longueuil (Ville), 1997 CanLII 335 (S.C.C.) , [1997] 3 S.C.R., http://www.canlii.org/en/ca/scc/doc/1997/1997canlii335/1997canlii335.html.

Google Spain SL, Google Inc. v Agencia Española de Protección de Datos, Mario Costeja González (2014) CJEU, http://curia.europa.eu/juris/document/document_print.jsf?doclang=EN&text&pageIndex=0&part=1&mode=DOC&docid=152065&occ=first&dir&cid=437838.

Greenleaf, Graham, "The Australia Card: Towards a National Surveillance System" (October 2, 1987), Law Society Journal (NSW) Vol. 25, No. 9, October 1987, SSRN: http://ssrn.com/abstract=2195493.

Greenleaf, Graham, "Australia's Proposed ID Card: Still Quacking Like a Duck", UNSW Law Research Paper No. 2007-1; Computer Law & Security Report, Vol. 23, 2007, SSRN: http://ssrn.com/abstract=951358 or http://dx.doi.org/10.2139/ssrn.951358.

Hunter v. Southam Inc., [1984] 2 S.C.R. 145, http://www.canlii.org/en/ca/scc/doc/1984/1984canlii33/1984canlii33.html.

ICANN, Affirmation of Commitments by the United States Department of Commerce and the Internet Corporation for Assigned Names and Numbers https://www.icann.org/resources/pages/affirmation-of-commitments-2009-09-30-en.

ICANN, Final Report from the Expert Working Group on gTLD Directory Services: A Next Generation Registration Directory Service (RDS). June 6, 2014. https://www.icann.org/en/system/files/files/final-report-06jun14-en.pdf. Though not included in the report, a dissenting opinion was filed and can be found at http://www.internetgovernance.org/2014/06/07/icann-suppresses-a-privacy-advocates-dissent/.

Inland Revenue and EDS: Divorce Impossible? ComputerWeekly.com http://www.computerweekly.com/feature/Inland-Revenue-EDS-Divorce-Impossible.

International Working Group on data protection in telecommunications, Working Paper on Big Data and Privacy, Privacy principles under pressure in the age of Big Data analytics (2014), http://www.datenschutz-berlin.de/content/europa-international/international-working-group-on-data-protection-in-telecommunications-iwgdpt/working-papers-and-common-positions-adopted-by-the-working-group.

INVOLVE: For a Stronger Democracy, "Data Sharing Open Policy Process" (May 2014), http://www.involve.org.uk/blog/2014/05/02/data-sharing-open-policy-process/.

Jolate, Sumedha, "Copenhagen City: e-Government Change Agent" (11 January 2013), http://www.futuregov.asia/articles/copenhagen-city-e-government-change-agent.

Jolls, Christine, "Rationality and Consent in Privacy Law" (2008), http://www.law.yale.edu/documents/pdf/Faculty/Jolls_RationalityandConsentinPrivacyLaw.pdf.

Joseph Rowntree Charitable Trust, http://www.jrct.org.uk/.

Kerr, Ian, Jennifer Barrigar, Jacquelyn Burkell, Katie Black, "Soft Surveillance, Hard Consent" (2006) 6 *Personally Yours.*

Knox, C., "Paradoxes of Modernization: Unintended Consequences of Public Policy Reform" (2011), Ed. Helen Margetts, Perri 6 and Christopher Hood, Public Administration, 89: 1691–1693. doi: 10.1111/j.1467-9299.2011.01989.x.

Laming, William, Chair of the Climbie Inquiry, Report of the Victoria Climbie Inquiry, London, The Stationery Office (Jan 2003), https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/273183/5730.pdf.

Mas, Susana, "Cyberbullying Bill Surveillance Powers Alarm Ontario Privacy Watchdog", (21 May 2014), CBC http://www.cbc.ca/news/politics/cyberbullying-bill-surveillance-powers-alarm-ontario-privacy-watchdog-1.2649523.

Mas, Susana, "Cyberbullying Victims' Parents Divided Over Privacy Concerns in Online Bill" (13 May 2014), CBC http://www.cbc.ca/news/politics/cyberbullying-victims-parents-divided-over-privacy-concerns-in-online-bill-1.2641104.

Milberry, Kate & Parsons, Christopher, A National ID Card by Stealth? The BC Services Card: Privacy Risks, Opportunities and Alternatives, BC Civil Liberties Association, (2013) http://www.christopher-parsons.com/Main/wp-content/uploads/2013/11/2013-National-ID-Card-by-Stealth.pdf.

Moule, Lawrence, "Lac Carling X: A Turning Point" (31 July 2006), ITWorld.com http://www.itworldcanada.com/article/lac-carling-x-a-turning-point/633#ixzz3BL4ppBgK.

Municipal Information Systems Association of Canada, http://www.misa-asim.ca/.

National Science Foundation, Solicitation 12-499: Core Techniques and Technologies for Advancing Big Data Science & Engineering (BIGDATA), (2012), http://www.nsf.gov/pubs/2012/nsf12499/nsf12499.pdf.

OECD, Denmark: Efficient e-Government for Smarter Public Service Delivery, OECD Publishing, http://www.oecd-ilibrary.org/governance/denmark-efficient-e-government-for-smarter-public-service-delivery_9789264087118-en.

OECD, Guidelines on the Protection of Privacy and Transborder Flows of Personal Data, http://www.oecd.org/internet/ieconomy/oecdguidelinesontheprotectionofprivacyandtransborderflowsofpersonaldata.htm.

OECD, Observatory of Public Sector Innovation: Country Profiles, Canada. https://www.oecd.org/governance/observatory-public-sector-innovation/countryprofiles/canada/

OECD, Recommendation on Digital Government Strategies (July, 2014), http://www.oecd.org/gov/public-innovation/recommendation-on-digital-government-strategies.htm.

OECD, Rethinking e-Government Services: User-Centred Approaches (2009), Approved OECD Governance Committee October 2008, http://www.oecd.org/gov/public-innovation/rethinkinge-governmentservicesuser-centredapproaches.htm.

O'Harrow, Robert, *No Place to Hide* (New York, Free Press, 2005).

Privacy Act (Can.) (Re), [1999] 2 FC 543, 1999 CanLII 9335 (FC), http://canlii.ca/t/48kq.

Privacy Act (Can.) (Re), [2000] 3 FC 82, 2000 CanLII 17110 (FCA), http://canlii.ca/t/4l8r.

Privacy Act (Can.) (Re.), [2001] 3 S.C.R. 905, 2001 SCC 89: http://www.canlii.org/en/ca/fca/doc/1998/1998canlii9071/1998canlii9071.html.

Reding, Vivianne, Vice-President of the European Commission: Protecting EU citizens' data from mass surveillance (speech 11 March 2014), http://ec.europa.eu/commission_2010-2014/reding/multimedia/news/2014/05/20140531_en.htm; http://europa.eu/rapid/press-release_SPEECH-14-209_en.htm.

RWDSU v. Dolphin Delivery Ltd., [1986] 2 S.C.R. 573.

R. v. Edwards, [1996] 1 S.C.R. 126, http://scc-csc.lexum.com/scc-csc/scc-csc/en/item/1340/index.do.

R v. Gomboc 2010 SCC 55, http://scc-csc.lexum.com/scc-csc/scc-csc/en/item/7898/index.do.

R. v. Kang-Brown, 2008 SCC 18, http://scc-csc.lexum.com/scc-csc/scc-csc/en/item/4627/index.do.

R. v. Malmo-Levine, 2003 SCC 74 (CanLII) , http://www.canlii.org/en/ca/scc/doc/2003/2003scc74/2003scc74.html, [2003] 3 S.C.R. 571.

R v. Morgentaler, 1988 CanLII 90 (S.C.C.) , [1988] 1 S.C.R. 30, http://www.canlii.org/en/ca/scc/doc/1988/1988canlii90/1988canlii90.html.

R. v. O'Connor, 1995 CanLII 51 (S.C.C.), wwww.canlii.org/en/ca/scc/doc/1995/1995canlii51/1995canlii51.pdf.

R. v. Plant, [1993] 3 S.C.R. 281, http://www.canlii.org/en/ca/scc/doc/1993/1993canlii70/1993canlii70.html.

R. v. Rahey [1987] 1 S.C.R. 588, http://www.canlii.org/en/ca/scc/doc/1987/1987canlii52/1987canlii52.html.

R. v. S.A.B., 2003 SCC 60, 2003 SCC 60, http://www.canlii.org/en/ca/scc/doc/2003/2003scc60/2003scc60.html.

R v. Spencer, [2014] SCC 43, 2014] SCC 43, http://scc-csc.lexum.com/scc-csc/scc-csc/en/item/14233/index.do.

R. v. Tessling, [2004] 3 S.C.R. 432, http://scc-csc.lexum.com/scc-csc/scc-csc/en/item/2183/index.do.

Records Maintained on Individuals: Public Law 93-579, 5 U.S.C. § 552a, http://www.law.cornell.edu/uscode/text/5/552a.

Schaar, Peter, "The Internet and Big Data - Incompatible with Data Protection?" (2014), *MIND: Collaborative Discussion Paper Series #1*; 7 Privacy and Internet Governance 14. http://www.collaboratory.de/images/1/11/PrivacyandInternetGovernanceMIND7.pdf.

Schwartz, Paul M., "Privacy and Democracy in Cyberspace", 52 *Vanderbilt Law Review* 1607 (1999) http://works.bepress.com/paul_schwartz/7/.

Smith v. Canada (Attorney General), 2000 CanLII 14930 (FCA), http://canlii.ca/t/4ld3.

Smith v. Canada (Attorney General), [2001] 3 S.C.R. 902, 2001 SCC 88:P https://scc-csc.lexum.com/scc-csc/scc-csc/en/item/1930/index.do.

Smith, Robert Ellis, *Ben Franklin's Web Site: Privacy and Curiosity from Plymouth Rock to the Internet*, (Privacy Journal, 2004).

Steele, Chandra, "The 10 Most Disturbing Snowden Revelations" (11 Feb 2014), PC Mag http://www.pcmag.com/article2/0,2817,2453128,00.asp.

Tay, Liz, "Centrelink's data centre plans spark privacy concerns: IT News for Australian Business" (June 2010), http://www.itnews.com.au/News/213723,centrelinks-data-centre-plans-spark-privacy-concerns.aspx.

United Kingdom, Cabinet Office, Draft policy proposals for Tailored Public Services (dated 28th July 2014), https://docs.google.com/document/d/1g6kpiRUpgECnR2IXCuP0O1_VmuMMBgbD-oCmQI4wHVE/edit?pli=1.

United Kingdom, Department of Health, The Caldicott Committee Report on the Review of Patient-Identifiable Information (December 1997), Chairman Fiona Caldicott, http://webarchive.nationalarchives.gov.uk/+/www.dh.gov.uk/en/Publicationsandstatistics/Publications/PublicationspolicyandGuidance/DH_4068403.

United Kingdom, Department of Health, Information: To share or not to share? The Information Governance Review (March 2013), Chairman Fiona Caldicott, http://www.hsj.co.uk/Journals/2013/04/25/r/a/k/The-Information-Governance-Review-Report.pdf.

United Kingdom, Information Commissioner's Office, Data sharing code of practice (May 2011), http://ico.org.uk/for_organisations/data_protection/topic_guides/~/media/documents/library/Data_Protection/Detailed_specialist_guides/data_sharing_code_of_practice.ashx.

United Kingdom, Information Commissioner's Office, ICO Response to Law Commission Data Sharing Between Public Bodies Consultation (December 2013), http://ico.org.uk/about_us/consultations/~/media/documents/consultation_responses/ICO-response-to-Law-Commission-Data-Sharing-consultation.pdf .

United Kingdom, Law Commission, Data Sharing Rules Must be Reformed (11 July 2014), http://lawcommission.justice.gov.uk/news/2842.htm.

United Kingdom, Law Commission, Data Sharing Between Public Bodies (11 July 2014), http://lawcommission.justice.gov.uk/publications/2811.htm.

United Kingdom, Law Commission, Data Sharing Between Public Bodies: A Consultation Paper (2013) (Consultation Paper No. 214), http://lawcommission.justice.gov.uk/docs/cp214_data-sharing.pdf.

United Kingdom, Law Commission, *Data Sharing Between Public Bodies: A Scoping Report* (Law Commission No. 351), presented to UK Parliament 9/10/2014, http://lawcommission.justice.gov.uk/docs/lc351_data-sharing.pdf.

United Nations High Commissioner for Human Rights, The Right to Privacy in the Digital Age (30 June 2014), http://www.ohchr.org/en/hrbodies/hrc/regularsessions/session27/documents/a.hrc.27.37_en.pdf.

U.S. *Computer Matching and Privacy Protection Act of 1988*: Public Law 100-503, 102 Stat. 2507, http://www.gpo.gov/fdsys/pkg/STATUTE-102/pdf/STATUTE-102-Pg2507.pdf.

U.S. Department of Health, Education & Welfare, *Records, Computers and the Rights of Citizens*, Report of the Secretary's Advisory Committee on Automated Personal Data Systems (U.S. Department of Health, Education & Welfare, 1973), http://epic.org/privacy/hew1973report/default.html

U.S. Department of Homeland Security, DHS *Information Sharing and Safeguarding Strategy* (2013), http://www.dhs.gov/sites/default/files/publications/12-4466-dhs-information-sharing-and-safeguarding-strategy-01-30-13--fina%20%20%20.pdf.

U.S. Department of Homeland Security, *Privacy Impact Assessment for the DHS Data Framework* (2013) (DHS/ALL/PIA-046), http://www.dhs.gov/sites/default/files/publications/privacy-pia-dhs-wide-dhsdataframework-11062013.pdf.

U.S. Executive Office of the President, Big Data: Seizing Opportunities, Preserving Values (2014), http://www.whitehouse.gov/sites/default/files/docs/big data_privacy_report_5.1.14_final_print.pdf.

U.S. Federal Trade Commission, Privacy Online: Fair Information Practices in the Electronic Marketplace: A Report to Congress" (1998), http://www.ftc.gov/sites/default/files/documents/public_events/exploring-privacy-roundtable-series/priv-23a.pdf .

U.S. Government Accountability Office, Government Accountability Act, Computer Matching Act: OMB and Selected Agencies Need to Ensure Consistent Implementation (2014) (GAO-14-44), http://gao.gov/products/GAO-14-44.

U.S. *Income Tax Code*; 26 U.S.C. § 6103, http://www.law.cornell.edu/uscode/text/26/6103.

U.S. Internal Revenue Service, Safeguards Programs (16 July 2014), http://www.irs.gov/uac/Safeguards-Program.

U.S. Internal Revenue Service, *Tax Information Security Guidelines for Federal, State and Local Agencies* (Publication 1075), http://www.irs.gov/file_source/pub/irs-pdf/p1075.pdf.

U.S. National Institute of Standards and Technology, nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r4.pdf; now replaced by new draft: http://csrc.nist.gov/publications/drafts/800-161/sp800_161_2nd_draft.pdf.

U.S. National Institute of Standards and Technology, csrc.nist.gov/publications/nistpubs/800-30-rev1/sp800_30_r1.pdf.

U.S. Office of the Press Secretary: White House, Fact Sheet: Big Data and Privacy Working Group Review (1 May 2014), http://www.whitehouse.gov/the-press-office/2014/05/01/fact-sheet-big-data-and-privacy-working-group-review.

U.S. *Privacy Act of 1974*: Public Law 93-579, 5 U.S.C. § 552a, http://www.law.cornell.edu/uscode/text/5/552a.

U.S. Public Law: *Federal Parent Locator Service*: 42 U.S.C.§§ 653, 653a, http://www.law.cornell.edu/uscode/text/42/653.

U.S. Treasury Inspector General for Tax Administration, While Effective Actions Have Been Taken to Address Previously Reported Weaknesses in the Protection of Federal Tax Information at State Government Agencies, Additional Improvements Are Needed (2009) (Reference Number: 2010-20-003), http://www.treasury.gov/tigta/auditreports/2010reports/201020003fr.pdf.

World Economic Forum, *Personal Data: the Emergence of a New Asset Class* (2011), http://www3.weforum.org/docs/WEF_ITTC_PersonalDataNewAsset_Report_2011.pdf.

World Economic Forum, *Rethinking Personal Data: Strengthening Trust* (2012), http://www3.weforum.org/docs/WEF_IT_RethinkingPersonalData_Report_2012.pdf.

World Economic Forum, *Rethinking Personal Data, a New Lens for Strengthening Trust* (2014), http://www3.weforum.org/docs/WEF_RethinkingPersonalData_ANewLens_Report_2014.pdf.

World Economic Forum, *The Internet Trust Bubble: Global Values, Beliefs and Practices* (2014), http://www3.weforum.org/docs/WEF_InternetTrustBubble_Report2_2014.pdf.

Zalnieriute, M. & Schneider, T., *ICANN's procedures and policies in the light of human rights, fundamental freedoms and democratic values* (2014), DGI(2014)12. Strasbourg, France: Council of Europe, http://www.academia.edu/7495980/ICANNs_procedures_and_policies_in_the_light_of_human_rights_fundamental_freedoms_and_democratic_values.

Zittrain, J. "Is the EU Compelling Google to Become About Me?" (May 2014), Blog: Future of the Internet and How to Stop It. http://blogs.law.harvard.edu/futureoftheinternet/2014/05/13/is-the-eu-compelling-google-to-become-about-me/.

Authors' Biographies

Stephanie Perrin

Since 1984, Ms. Perrin has devoted most of her career to information and privacy issues, having started as one of the first federal Access to Information and Privacy Coordinators at the then-Department of Communications. For ten years, she worked as a policy analyst for the Department of Communications and Industry Canada, developing the Canadian Standard for the Protection of Personal Information and incorporating it in law as the *Personal Information Protection and Electronic Documents Act* (PIPEDA) for the private sector. She also represented Canada at the Organisation for Economic Co-operation and Development on the committee dealing with privacy and security issues, and worked in the private sector as Chief Privacy Officer for Zero Knowledge Systems. She has held the positions of Director of Policy and Research at the Office of the Privacy Commissioner and Director of Risk Management Policy for Service Canada. Most recently, she has re-launched Digital Discretion Inc. which she initially started in 2003.

Ms. Perrin graduated from Carleton University with an MA, and is now a doctoral candidate at the Faculty of Information at the University of Toronto, where she is researching issues influencing online privacy protection. .

Dr. Jennifer Barrigar

Dr. Barrigar is a legal scholar and writer on privacy and reputation. For several years she served as Legal Counsel at the Office of the Privacy Commissioner of Canada where she participated in the initial application and interpretation of Canada's private sector law, as well as working with international standards for privacy and data protection. She has also taught law courses at the University of Ottawa and Carleton University.

Dr. Barrigar holds LL.D and LL.M. degrees from the University of Ottawa, working with the Centre for Law, Technology and Society. She also holds an LL.B. from Dalhousie University and a BA (Honours) from Carleton University.

Robert Gellman

Mr. Gellman worked for 17 years on the staff of the Subcommittee on Government Information of the U.S. House Committee on Government Operations. During that time, he was responsible for all information policy activities including privacy, the *Privacy Act of 1974,* health privacy, the collection and dissemination of electronic data, the *Freedom of Information Act* and other matters. From 1996 to 2000, Bob was a member of the National Committee on Vital and Health Statistics, an advisory committee of the U.S. Health and Human Services Department. He chaired its Subcommittee on Privacy and Confidentiality from 1996 to 1998.

Since 1995, Mr. Gellman has also worked as a privacy and information policy consultant with clients that included large and small companies, trade associations, government agencies (U.S. and others), NGOs and privacy advocacy organizations. He has been a member of the Editorial Board of Government Information Quarterly since 1996, and in 2012, he was named Senior Fellow at the Center on Law and Information Policy, at the Fordham University School of Law.

He holds a BA from the University of Pennsylvania and a JD from the Yale Law School.

Heather Black

Ms. Black is a Senior Consultant with Digital Discretion. Although she was not a principal author, she was consulted for her expertise on this research project, and the authors wish to thank her for her contribution.

Ms. Black is a graduate in English from Sir George Williams University (now part of Concordia University), and in common law from McGill University. She was called to the Ontario Bar in 1976.

She practised law in the federal Department of Justice from 1976 to 2000, specializing in commercial, and information and privacy law. Beginning in 1982, when she worked on the implementation of the federal access to information and privacy legislation, Ms. Black acquired extensive experience in information and privacy law. In the mid-1990s she began work with Stephanie Perrin on the project that ultimately culminated in the drafting and passage of the *Personal Information Protection and Electronic Documents Act* (PIPEDA) in 2000. She co-authored *The Personal Information Protection and Electronic Documents Act: An Annotated Guide* with Stephanie Perrin, David Flaherty and Murray Rankin. The guide was published in 2001 by Irwin Law.

In 2000, Ms. Black joined the Office of the Privacy Commissioner of Canada (OPC). A year later, she was appointed General Counsel at the OPC and, in 2003, was promoted to Assistant Commissioner with primary responsibility for private sector privacy. She retired from the public service in 2007 and has since been working as a consultant, including being a member of the External Advisory Board for the Office of the Information and Privacy Commissioner of British Columbia.