CANADA REPORT

Big Data Technology and National Security

Comparative International Perspectives on
Strategy, Policy and Law

Law and Policy Program
Data to Decisions Cooperative Research Centre

June 2018

Research Team
Professor Louis de Koker, Program Leader
Professor Janet Chan, Project Leader
Professor Danuta Mendelson, Key Researcher
Associate Professor Lyria Bennett Moses, Key Researcher
Dr Alana Maurushat, Key Researcher
Mr David Vaile, Key Researcher
Mr Mike Gaffney, Researcher
Mr Gregory Sadler, Researcher
Mr Patrick Grierson, Researcher
Mr Daniel Cater, Project Research Assistant

Other research assistants
Ms Alana James
Ms Sonam Gordhan
Mr Jax Arnold

Interns (in alphabetical order)
Ms Kendy Ding
Mr Ciaran Finnane
Ms Monica Ma
Mr Kevin Tsu
Mr Atul Vidhata
Mr Vincent Wan
Ms Jacqueline Yip

Canada Report

Principal author and interviews
Dr Alana Maurushat

Research assistance
Mr Daniel Cater

Qualitative analysis
Lyria Bennett Moses

Technical editing
Mr David Vaile

Other Reports from this Project

Methodology Report
Australia Report
UK Report
Comparative Report

Select Bibliography
Technical References [for Australia Report]
## Table of contents

List of Tables ......................................................................................................................... iv

1. THE CANADIAN LEGAL CONTEXT ................................................................................. 1
   1.1 Intelligence and national Security – contours of the policy discussion .................. 1
   1.2 National intelligence and law enforcement agencies .............................................. 2
   1.3 Selection of agencies and laws for purposes of this study ........................................ 8
   1.4 Leading case law on Sections 7 and 8 of the Canadian *Charter of Human Rights and Freedoms* ........................................................................................................ 10
   1.5 Reports and Frameworks .......................................................................................... 16

2. USING BIG DATA FOR NATIONAL SECURITY: STAKEHOLDERS’ PERSPECTIVES ........ 18
   2.1 Current Use of Data .................................................................................................. 18
   2.2 Current concerns regarding access to and sharing of data ..................................... 23
   2.3 How problems can be overcome ............................................................................ 25
   2.4 Big Data: potentials, limits and risks ..................................................................... 28
   2.5 Regulation ............................................................................................................... 37
   2.6 Values and Big Data ............................................................................................... 45

3. BIG DATA, LAW ENFORCEMENT AND NATIONAL SECURITY: THE LEGAL ENVIRONMENT IN CANADA ..................................................................................... 51
   3.1 Is access for data mining enabled and are legal controls comprehensive and proportionate? ........................................................................................................ 51
   3.2 Are legal controls comprehensive and proportional? ............................................. 67
   3.3 Are legal rules clear, principle-based, consistent and instructive? ....................... 67
   3.4 Is integrity of data and analysis supported? ........................................................... 69
   3.5 Are data and systems protected? ........................................................................... 72
   3.6 Is accountability maintained? ............................................................................... 75
   3.7 Are principles and rules regularly reviewed? ......................................................... 81
   3.8 Is there a sufficient measure of transparency? ...................................................... 82

4. Conclusion ......................................................................................................................... 85
   4.1 Using Big Data for national security: Stakeholders’ perspectives ......................... 85
   4.2 Big Data, law enforcement and national security: The legal environment in Canada ......................................................................................................................... 91

Appendix ................................................................................................................................ 97
   A. Interviews with law enforcement and intelligence officials – Canada .................... 97
   B. Interviews with technologists/designers – Canada .................................................. 100
   C. Interviews with policymakers, citizen groups – Canada ......................................... 103
List of Tables

Table 1-1: Law Enforcement and National Security Agencies in Canada........................ 3
Table 1-2: Summary of Key Cases Interpreting and Restricting Data Access, Use and Disclosure .................................................................................................................. 12
Table 2-1 General Attitudes towards Computer Technology (n=6).............................. 18
Table 2-2: Type of Data Used by Nature of Organisation (n=3)................................. 19
Table 2-3: Sharing of Data between Canadian Organisations ................................... 20
Table 2-4: Current Concerns re Access to and Sharing of Data by Role in Organisations (n=6) .............................................................................................................. 23
Table 2-5: Current Concerns by How Problems Can Be Overcome (n=6)............... 25
Table 2-6: Conception of Big Data by Role and Type of Organisation (n=11)........... 28
Table 2-7: Perceived Capability of Big Data by Role and Type of Organisation (n=8) .......................................................... 29
Table 2-8: Use of Big Data by Type of Organisation (n=11) ..................................... 30
Table 2-9: Current Use of Data Analysis Tools by those in Operational Organisations (n=6) .................................................................................................................... 31
Table 2-10: Barriers/Challenges to use of Big Data by Type of Organisation (n=11) .............................................................................................................................. 32
Table 2-11: Risks of Using Big Data by Role of Organisation (n=11) ...................... 33
Table 2-12: Who is exposed to risks of Big Data by Organisation of Participant (n=11) ........................................................................................................................... 36
Table 2-13: How Big Data Risks can be Managed (n=11) .................................... 36
Table 2-14: Legislation and regulatory material identified by research participants according to (1) organisation sector, and (2) type of role and organisation (n=11) ........................................................................................................ 38
Table 2-15: Evaluation of appropriateness and effectiveness of laws, regulation and oversight by research participants by (1) sector of organisation and (2) type of organisation (n=11) .................................................................................. 41
Table 2-16: Mitigation of issues/risks associated with data analytics/storage systems through design (n=3) .................................................................................... 44
Table 2-17: Policy participants’ attitudes to privacy by organisation sector .......... 46
Table 2-18: Responses to general kidnapping scenario and specific prompts (n=5) ................................................................................................................................. 47
Table 2-19: Transparency ......................................................................................... 48
Table 2-20: Sources of views of Policy group by organisation sector ................. 50
1. THE CANADIAN LEGAL CONTEXT

1.1 Intelligence and national Security – contours of the policy discussion

The Canadian national security landscape is diverse with various government agencies having separate or concurrent jurisdiction over matters related to national security. Canada’s lead intelligence agency, the Canadian Security Intelligence Service (CSIS) has a mandate to perform domestic intelligence services while the Communications Security Establishment (CSE) performs international intelligence services and falls under the Department of Defence. Both CSIS and CSE have traditionally not had the power to take law enforcement measures against a threat – this is largely the responsibility of the Royal Canadian Mounted Police (RCMP).

While there have been many controversial bills introduced in Parliament over the history of Canada, the recently introduced Bill C-51 (this is the colloquial reference and also what has been used in the media, in reports and other instruments) has arguably been one of the most controversial bills passed into law. The bill is referred to as C-51 and not its name as it was introduced as an Omnibus bill. The Omnibus bill was a single document containing very dense, lengthy and complex legislative amendments to several Acts. The official name is the Anti-Terrorism Act 2015 which enacted the Security of Canada Information Sharing Act and the Secure Air Travel Act, amended the Criminal Code, the Canadian Security Intelligence Service Act and the Immigration and Refugee Protection Act and made related and consequential amendments to other Acts.

The main focus of C-51 was to amend the Anti-Terrorism Act; this led to a number of concerns which will be summarised below. The bill also led to the enactment of a new piece of legislation, the Security of Canada Information Sharing Act 2015 (SCISA). The bill was introduced quickly after the shooting incidents in Parliament Hill in Ottawa and those in Montreal. The size and scope of such Omnibus bills limits the ability of Parliament to debate the issues adequately. The bill was not given a Second Reading in Parliament.

In this case, the media and various organisations were quick to point out the lack of debate on what some have hailed as a significant impediment to privacy, freedom of expression and civil liberties in general – all heightened due to the public’s knowledge acquired through the Snowden revelations. One commentator has argued that C-51 stands out as the singular example of the style of government under the Conservative Harper government that affected the past decade, and this feature is what makes the bill so controversial and unique.

---


A number of additional concerns were raised by prominent lawyers and experts:

- The expansive definition of ‘threats to the security of Canada’ under s 2(b) SCISA
- The expansion of CSIS powers to include powers similar to law enforcement powers of the RCMP
- Warrants are only required to access, use and disclose information of a non-citizen if a *Charter of Human Rights* breach would occur. This new framework is contrary to how both warrants and the Charter normally work. Generally, you need a warrant to obtain information for investigations leading to criminal charges where the subject is a non-citizen present in Canada. The courts have not granted Charter rights to non-citizens and therefore the Charter will not be violated if data is in relation to a non-citizen present in Canada.
- The warrant process is secret
- The current security oversight review body known as Security Intelligence Review Committee is weak
- Overbroad definitions of ‘terrorism offences’ and ‘terrorist propaganda’
- Overbroad definition of ‘security interest’ or ‘threat’ allowing for sharing between agencies where there is any ‘activity that undermines the security of Canada’
- No mandatory information sharing requirements between the two main entities in national security, the RCMP and CSIS
- The appeal provisions are limited with limited ability for adversarial challenge of intelligence and evidence acquired through secrecy
- No mandatory review of its operations and unintended mishaps.

Privacy protection has not been enhanced as contrary to special report and enquiries. Some of these concerns are expected to be addressed when the *Anti-Terrorism Act* is amended in 2016 by the new government led by Prime Minister Justin Trudeau. Though no amendments have yet been tabled, the new Liberal government made election promises to amend the controversial bill (C-51) to be more privacy oriented, less broad, and with better oversight mechanisms.

### 1.2 National intelligence and law enforcement agencies

Table 1-1 outlines the agencies involved in national security and law enforcement, their responsibilities and enabling legislation. It is important to note that Canada categorises agencies based on the broader notion of ‘security threat’ as opposed to ‘national security’...
threat’, leading to information sharing between agencies not typically associated with law enforcement or intelligence such as the Canadian Food Inspection Agency.

Table 1-1: Law Enforcement and National Security Agencies in Canada

<table>
<thead>
<tr>
<th>AGENCY</th>
<th>BRIEF OVERVIEW OF RESPONSIBILITIES</th>
<th>ENABLING LEGISLATION</th>
<th>SUBJECT TO SCISA</th>
</tr>
</thead>
<tbody>
<tr>
<td>Royal Canadian Mounted Police (RCMP)</td>
<td>• Customs and excise</td>
<td>Royal Canadian Mounted Police Act (R.S.C. 1985, c. R-10)</td>
<td>Yes</td>
</tr>
<tr>
<td></td>
<td>• Drug Enforcement</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Economic Crime</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Federal Policing</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Immigration</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Proceeds of Crime</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Criminal Intelligence</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>• International Liaison and Protective Services</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Provincial police</td>
<td>• Responding to municipal police requests for special assistance in emergencies</td>
<td>e.g. the Ontario Provincial Police Act (R.S.O. 1990, c. P.15)</td>
<td>No</td>
</tr>
<tr>
<td></td>
<td>• Providing traffic control</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Investigative services on request to the Coroner’s Office and to other police ministries</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Performing other assigned duties such as maintaining the provincial firearms registry, providing security and protecting government officials and dignitaries.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Municipal Police (in all cities, e.g. Toronto Metropolitan Police)</td>
<td>• Preserving the peace</td>
<td>Under a provincial Act of each municipality e.g. Ontario’s Police Services Act, ss 4 and 5, a municipality must assume responsibility for its police services when, as a result of the Canadian census, its population reaches a certain number.</td>
<td>No</td>
</tr>
<tr>
<td></td>
<td>• Prevention of crimes</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Assisting victims of crime</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Apprehending criminals</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Laying charges and participating in prosecutions</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Enforcing municipal bylaws</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Executing warrants</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

*Security of Canada Information Sharing Act.*
<table>
<thead>
<tr>
<th>AGENCY</th>
<th>BRIEF OVERVIEW OF RESPONSIBILITIES</th>
<th>ENABLING LEGISLATION</th>
<th>SUBJECT TO SCISA¹</th>
</tr>
</thead>
</table>
| Canadian Security Intelligence Service (CSIS) | • Investigation of activities suspected of constituting threats to the security of Canada, and to report on these to the Government of Canada.  
• Collection and analysis of threat-related information, which is typically disseminated to government partners;  
• Key threats include terrorism, the proliferation of weapons of mass destruction, espionage, foreign interference and cyber-tampering affecting critical infrastructure. CSIS programs are proactive and pre-emptive.  
• Through its Security Screening Program, prevention of non-Canadians who pose security concerns from entering Canada or receiving permanent resident status or citizenship.  
• Safeguarding the confidential information of the Government of Canada from foreign governments and other entities that may present a risk.  
• Countering terrorist violence is the top priority for CSIS. | Canadian Security Intelligence Service Act (R.S.C. 1985, c. C-23) | Yes |
| Communications Security Establishment (CSE) | • Acquiring and using information from the global information infrastructure for the purpose of providing foreign intelligence, in accordance with the Government of Canada intelligence priorities;  
• Providing advice, guidance and services to help ensure the protection of electronic information and information infrastructures of importance to the Government of Canada; and  
• Providing technical and operational assistance to federal law enforcement and security agencies in the performance of their lawful duties. | National Defence Act (R.S.C. 1985, c. N-5) | Yes |
| Department of Foreign Affairs, Trade and Development (DFAIT – T&D) | • Foreign Relations  
• International Trade  
• Consular Services  
• International Development  
• Humanitarian Assistance  
• Reports on Human Rights in various countries | Department of Foreign Affairs, Trade and Development Act (S.C. 2013, c. 33, s 174) | Yes |
| Department of National Defence (DOD) | • Protection of Canada  
• Defence of North America in co-operation with US  
| Privy Council Office | • Objective policy advice and information to support the Prime Minister and Cabinet;  
• Consultation and collaboration with international and domestic sources inside and outside government (including provinces and territories)  
• Information on the priorities of Canadians | Constitutional Act, 1867 | No |
<table>
<thead>
<tr>
<th>AGENCY</th>
<th>BRIEF OVERVIEW OF RESPONSIBILITIES</th>
<th>ENABLING LEGISLATION</th>
<th>SUBJECT TO SCISA</th>
</tr>
</thead>
</table>
| Canada Border Services Agency (CBSA) | - Administering legislation that governs the admissibility of people and goods, plants and animals into and out of Canada;  
- Detaining those people who may pose a threat to Canada;  
- Removing people who are inadmissible to Canada, including those involved in terrorism, organized crime, war crimes or crimes against humanity;  
- Interdicting illegal goods entering or leaving the country;  
- Promoting Canadian business and economic benefits by administering trade legislation and trade agreements to meet Canada's international obligations;  
- Collecting applicable duties and taxes on imported goods. | Canada Border Services Agency Act (S.C. 2005, c. 38) | Yes |
| Department of Finance (Dept Fin) | - Preparing the federal budget.  
- Preparing tax and tariff legislation.  
- Managing federal borrowing on financial markets.  
- Administering major federal transfers to the provinces and territories.  
- Developing regulatory policy for financial sector.  
- Representing Canada within international financial institutions. | Financial Administration Act (R.S.C. 1985, c. F-11) | Yes |
| Financial Transactions and Reports Analysis Centre of Canada (FTRACC) | - Facilitating the detection, prevention and deterrence of money laundering and the financing of terrorist activities;  
- Ensuring compliance of reporting entities with the legislation and regulations;  
- Producing financial intelligence relevant to money laundering, terrorist activity financing and threats to the security of Canada investigations;  
- Maintaining a registry of money services businesses in Canada;  
- Enhancing public awareness and understanding of money laundering and terrorist activity financing. | Proceeds of Crime (Money Laundering) and Terrorist Financing Act (S.C. 2000, c. 17) | Yes |
| Canada Revenue Agency (CRA) | - Administration of tax laws for the Government of Canada and for most provinces and territories;  
- Administration of various social and economic benefit and incentive programs delivered through the tax system. | Canada Revenue Agency Act (S.C. 1999, c. 17) | Yes |
| Canadian Armed Forces (CAF) | - Patrolling Canada’s coasts and monitoring Canada’s skies  
- Leading search and rescue missions  
- Assisting civilian rescue authorities with disaster relief (forest fires, floods, avalanches, hurricanes, etc.) | National Defence Act (R.S.C., 1985, c. N-5) | Yes |
<table>
<thead>
<tr>
<th>AGENCY</th>
<th>BRIEF OVERVIEW OF RESPONSIBILITIES</th>
<th>ENABLING LEGISLATION</th>
<th>SUBJECT TO SCISA?</th>
</tr>
</thead>
</table>
| Canada Food Inspection Agency (CFIA) | • Establishing policies and standards for the safety and nutritional quality of food sold in Canada;  
• Administration of those provisions of the Canadian Food and Drugs Act that relate to public health, safety and nutrition;  
• Assessing the effectiveness of the Agency’s activities related to food safety. | Canadian Food Inspection Agency Act (S.C. 1997, c. 6) | Yes |
| Canadian Nuclear Safety (CNS) | • Regulation of the development, production and use of nuclear energy in Canada to protect, health, safety and the environment.  
• Implementation of measures respecting international control of the development, production, transport and use of nuclear weapons and nuclear explosive devices  
• Dissemination of scientific, technical and regulatory information concerning the activities of the CNSC, and the effects on the environment, on the health and safety of persons. | Nuclear Safety and Control Act (S.C. 1997, c. 9) | Yes |
| Department of Citizenship and Immigration (Dept. Imm) | • Facilitating the arrival of people and their integration into Canada;  
• Maintaining Canada’s humanitarian tradition by protecting refugees and people in need of protection;  
• Enhancing the values and promote the rights and responsibilities of Canadian citizenship; and  
• Advancing global migration policies in a way that supports Canada’s immigration and humanitarian objectives. | Department of Citizenship and Immigration Act (S.C. 1994, c. 31) | Yes |
| Treasury Board of Canada (TBC) | • **Management Office** – promoting improved management performance and approving policies to support the prudent and effective management of the government’s assets, financial, information and technology resources.  
• **Budget Office** – examining and approving the proposed spending plans of government departments, and reviewing the development of approved programs.  
• **People Management Office** – setting people management policies and managing compensation and labour relations, including determining the terms and conditions of employment | There is no one piece of enabling legislation for the Treasury Board. Its mission and powers are derived from a number of enabling laws:  
• Auditor General Act  
(R.S.C. 1985, c. A-17)  
• Governor General’s Act (R.S.C. 1985, c. G-9)  
• Financial Administration Act (R.S.C. 1985, c. F-11) | No |

---

<table>
<thead>
<tr>
<th>AGENCY</th>
<th>BRIEF OVERVIEW OF RESPONSIBILITIES</th>
<th>ENABLING LEGISLATION</th>
<th>SUBJECT TO SCISA*</th>
</tr>
</thead>
</table>
| Auditor General  | • Auditing the federal government, including some 100 departments and agencies, ranging from small boards to large, complex organizations whose activities extend across Canada and overseas; 40 Crown corporations, such as the Canadian Broadcasting Corporation and the Royal Canadian Mint; and the governments of Nunavut, the Yukon, the Northwest Territories, and some 20 territorial corporations and agencies.  
• These audits are financial, performance or special examination. | Auditor General Act (R.S.C. 1985, c. A-17)                       | No               |
| Canada Post      | • Exclusive privilege in Canada of collecting, transmitting and delivering letters to addressee  
• Similar duties for the Board of Director of any privately held corporation  
• As the postal service is within the scope of critical infrastructure, Canada Post is exempted from many provisions in relation to access to information and privacy in the event of an emergency. | Canada Post Corporation Act (R.S.C. 1985, c. C-10)            | No               |

1.3 Selection of agencies and laws for purposes of this study

1.3.1 Agencies

In Canada, a large number of government agencies are legally authorised to share information under the Security of Canada Information Sharing Act 2015 (SCISA). While there are over 100 government departments and agencies entitled to share information, we have selected agencies most readily identified with security and also those that both generate and use large datasets. We have focused on the main agencies identified in SCISA with emphasis on four government agencies and one quasi non-government agency (not identified in the Act and therefore not allowed to share information as permissively as those agencies identified in the Sharing Act). These are: the RCMP, CSIS, CSE, DOD, and Canada Post (not identified in the Act).

Canada Post has been selected as it is a non-government agency; it is a Crown corporation and has cross-over with national security issues, but is regulated differently to traditional law enforcement and intelligence agencies. The purpose of its use is comparative, as it highlights the increasing blurring of responsibilities where security issues involve shared infrastructure (often critical) between government and private corporations.

1.3.2 Laws

While there are hundreds of applicable pieces of legislation in the Canadian national security context, we have selected to examine the most referred to Acts and frameworks as expressed in the interviews and identified in the literature and in media reports. These are:

- Privacy Act 1983
- Personal Information Protection and Electronic Documents Act 2000 (PIPEDA)

*Security of Canada Information Sharing Act.*
• **Access to Information Act 1985**
• **Security of Canada Information Sharing Act 2015**
• **Security Information Act 1985**
• Select portions of C-51 – the Anti-Terrorism Act 2015
• **Royal Canadian Mounted Police Act 1985 and Regulations**
• **Canadian Security Intelligence Service Act 1985 and Regulations**
• **Canadian Charter of Human Rights and Freedoms 1982**
• Enabling legislation for an agency or organisation (e.g. **Canada Post Corporation Act 1985**)
• **Audit General Act 1985**

Summaries of these Acts are not provided, but instead, relative principles and aspects of these instruments will be integrated with discussion of the Lens principles, identified in Chapter 5 of the Methodology Report, compared with Australia where appropriate in Chapters 2 and 3. The O’Connor Recommendations, the recommendations arising from the Iacobucci and O’Connor Inquiries, however, will be examined below separately as they have been identified by research participants as the cornerstone to how information should be shared and how national security incidences should be handled to best protect the public interest. Additionally, many of the O’Connor Recommendations stem from general principles found in much of Canadian law around law enforcement and intelligence gathering and the **Charter of Human Rights** such as proportionality, oversight, transparency, and the protection of human rights in general. This will be explored later below and in Chapter 3.

The Treasury Board of Canada sets Directives, Standards, Policies and Guidelines for Federal government agencies. While these policies and other frameworks are not legally binding in the sense that they are subject to penalty if breached, they are meant to provide guidance and act as a high level best practice instrument.

Some of the more relevant policies and directives for Big Data are:

• **Information Management Guidelines**
• **Identity Management**
• **Management of Information Technology Directive**
• **Metadata Standards**
• **Privacy and Web Analytics Standard**
• **Privacy Breaches Guidelines**
• **Privacy Impact Assessment Directive**
• **Privacy Practices Directive**
• **Privacy Protection Policy**
• **Privacy Requests and Correction of Personal Information Directive**
• **Proactive Disclosure**
• **Directive on Record-Keeping**
• **Open Government**
• **Operational Security: Management of Information Technology Security Standard**
• **Government Security Policy**
• **Integrated Risk Management Framework Taking Privacy into Account Before Making Contractual Decisions Guidance Document**

---

Memoranda of Understanding remain key agreements in the handling of cross-border investigations, intelligence sharing and data sharing in general, both between foreign entities, as well as between private organisations and government organisations. Law enforcement and intelligence agencies may enter into agreements where data is shared (providing the law doesn’t strictly prohibit sharing or similar operations). Memoranda of Understanding, however, are not publicly available documents and are rarely referred to by oversight bodies in their reports.

1.4 Leading case law on Sections 7 and 8 of the Canadian Charter of Human Rights and Freedoms

In addition to legislation, reports and policy frameworks Canada, unlike Australia, has had recent case law on intelligence gathering and law enforcement investigations involving data. The five main cases are Spencer, Jarvis, Wakeling, Telus, and Rogers. Spencer, Jarvis and Wakeling form a sections 7 and 8 Charter trilogy around the boundaries of permissible search and seizure laws when dealing with data. The Telus and Rogers cases provide additional guidance on section 8 of the Charter, as they do not consider s 7. They are considered briefly below and incorporated into the review of the Lens principles where appropriate.

Section 7 of the Canadian Charter of Human Rights and Freedoms states:

Life, liberty and security of person

7. Everyone 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.

Section 8 of the Canadian Charter of Human Rights and Freedoms states:

Search and seizure

8. Everyone has the right to be secure against unreasonable search or seizure.

As we will see below, Canadian Charter case law involving warrants to access, use and disclose information involves both sections 7 and 8 of the Charter.

The s 7 trilogy of Spencer, Jarvis and Wakeling addresses the limits of provisions that impact on the life, liberty and security of person. In these cases individuals charged with a crime raised objection to how law enforcement accessed, used and disclosed information about them arguing that this was done in a manner that interfered with life, liberty and security of person.

The Telus and Rogers decisions do not raise s 7 Charter issues as these decisions did not involve individuals accused of crimes but, rather, these were cases involving the Internet Service Providers challenging the validity of law enforcement request for large volumes of cellular traffic data.

All five decisions raised questions of the limits of s 8 of the Charter in the context of reasonable and lawful search and seizure. These cases also address when there is a reasonable expectation of privacy in a variety of contexts related to law enforcement agency’s use of information.

The courts have given precise direction in these five cases stating that if information is being accessed, used or disclosed as part of an investigation leading to criminal charges, there must be lawful authorisation. Lawful authorisation typically means requiring a warrant, and

10 R v Spencer [2014] 2 SCR 212.
more specifically, requiring the correct type of warrant for the information sought or with caveats and disclosure restrictions where appropriate.

In *R v Spencer*\textsuperscript{11} it was held that a valid warrant is required in order for an ISP to provide Internet Subscriber Information to help identify the individual connected to illegal activities (access and use of information).

In *R v Jarvis*\textsuperscript{12} it was held that the power of income tax authorities (CCRA) to require taxpayers to answer questions and to produce documents could not be used where the reason of the inquiry was to build a criminal case against the taxpayer. It was further held that a warrant issued under the Tax Act is essentially the same as a warrant issued under s.478 of the Criminal Code of Canada, and is valid for both the audit and investigative phases of a tax inquiry.

In *Wakeling v United States of America*\textsuperscript{13} the court discussed the boundaries of sharing information from a telecommunications intercept between Canadian and foreign authorities where they held that caveats and restrictions on information are required when there is a risk of an unfair trial, discrimination, political intimidation or where there would be human rights violations such as torture (disclosure of information).

In *R v Telus*\textsuperscript{14} it was held that in the advent of new technologies the police cannot use a general warrant to intercept a private communication. The most appropriate warrant must be used as Parliament established more rigorous and specific requirements for different warrant commensurate with the associated risk of privacy invasiveness.

*R v Rogers*\textsuperscript{15} established police guidelines for the issuance of Production Orders so that they are narrow and tailored so as not to unduly infringe upon the privacy of individuals as protection in s 8 of the *Charter*.

Table 1-2 below summarises key conceptions from these decisions related to controls on data.

---

\textsuperscript{11} *R v Spencer* [2014] 2 SCR 212.
\textsuperscript{12} *R v Jarvis* [2002] 3 SCR 757.
\textsuperscript{13} *Wakeling v United States of America* [2014] 3 SCR.
\textsuperscript{14} *R v Telus Communications Co* [2013] 2 SCR 3.
\textsuperscript{15} *R v Rogers Communications* [2016] ONSC 70.
Table 1-2: Summary of Key Cases Interpreting and Restricting Data Access, Use and Disclosure

<table>
<thead>
<tr>
<th></th>
<th>Data Access, Use and/or Disclosure</th>
<th>S 7 or S 8 of the Charter</th>
<th>Expectation of Privacy</th>
<th>Warrant Requirements</th>
</tr>
</thead>
<tbody>
<tr>
<td>Spencer</td>
<td>Data access and use</td>
<td>S 7 and 8</td>
<td>Yes</td>
<td>Yes for Internet subscriber information.</td>
</tr>
<tr>
<td>Jarvis</td>
<td>Data access and use</td>
<td>S 7 and 8</td>
<td>Yes</td>
<td>Yes for information from another government agency (e.g. Tax or Audit Authority) if requested for an investigation leading to criminal charges.</td>
</tr>
<tr>
<td>Wakeling</td>
<td>Data disclosure</td>
<td>S 7 and 8</td>
<td>Limited.</td>
<td>Warrant to intercept communications in Canada. Caveats and disclosure restrictions when sharing with foreign agency.</td>
</tr>
<tr>
<td>Telus</td>
<td></td>
<td>S 8</td>
<td>Yes</td>
<td>General warrant insufficient for intercept of private communication. Must use appropriate warrant even if imposes more restrictions and is more difficult to obtain.</td>
</tr>
<tr>
<td>Rogers</td>
<td></td>
<td>S 8</td>
<td>Yes</td>
<td>Production Orders must be done in a narrow and tailored manner to avoid infringing the privacy of innocent people.</td>
</tr>
</tbody>
</table>

More information and analysis about these cases is provided below. Some readers may want to skip the additional analysis and move to ‘Summary and Implications’ at the end of the analysis, and then to section 1.5.

*R v Spencer*

This case involved police obtaining subscriber information from an Internet Service Provider without a warrant. The policy requested that the ISP voluntarily provide subscriber information for an Internet account. The ISP provided this information. The information obtained led to the arrest and conviction of Mr. Spencer for possession of child pornography. At issue was whether the search and seizure conducted was a violation or privacy, and any other human rights under the *Charter of Human Rights*. The subscriber information was for the accused’s sister’s residence, and not that of the accused’s residence.

The Supreme Court of Canada developed a test for when there is the reasonable expectation of privacy and noted that the importance of the ‘totality of the circumstances and a large number of interrelated factors’. In this instance the court noted that Spencer had a subjective expectation of privacy, and that obtaining a subscriber’s information without judicial authority such as a warrant, was a violation of his rights as this constituted a search. Without such a warrant the search was deemed to be an act of unreasonable search and seizure in violation to s 8 of the *Charter of Human Rights and Freedoms*.16

---

16 It was further held that s 487.014 of the Criminal Code does not provide general investigative powers to obtain information without a warrant and that there is no lawful authority to do so under in s 7(3)(c.1)(ii).
**R v Jarvis**

This 2002 Supreme Court of Canada decision involved a tax audit where information was obtained without a warrant which led to an investigation of tax fraud and criminal charges being laid. Here the court required that there be lawful authority. Typically this has been in the form of a warrant that must be used when gathering information for an investigation where charges may be laid. In issuing its judgment, the court referenced privacy rights when establishing whether looking at data patterns constitutes a ‘search’ and therefore requires a warrant. Put another way, when identifying a group of individuals with traits that require further investigation and where this could lead to criminal charges, a warrant is required to both look at the data patterns, and then to use this information in the course of an investigation. Where there is an expectation of privacy, analysing a data set already under government control may require a warrant depending on data use. The Court differentiates between data usage for investigations as opposed to other uses (the Court does not discuss whether other uses would be intelligence as distinguished from criminal investigations). The Court does not discuss whether there is an expectation of privacy in relation to data already held by the government.

**Wakeling v United States of America**

The *Wakeling* decision involved a number of government entities including the Attorney General of Canada on behalf of the United States of America, The Attorney General of British Columbia, the Attorney General of Ontario, Attorney General of Quebec, the Canadian Civil Liberties Association, the British Columbia Civil Liberties Association, the Information Privacy Commissioner of Ontario and the Privacy Commissioner of Canada. The issues in *Wakeling* attracted many government organisations to make submissions signalling to the Court that the issues at hand were likely novel, and certainly controversial with many differing organisations with different vested interests.

Once again the issue of legal search and seizure was at the forefront. In this case the accused was plotting to transport drugs into the United States. Wakeling’s communications were the subject of an interception of communications. The information gleaned from the interceptions was shared with US authorities. The interceptions were shared without appropriate safeguards to ensure that the subject would not have his human rights violated. The defendant’s lawyers contended that disclosure of the information violates s. 7 and 8 of the *Canadian Charter of Human Rights* (the right to life, liberty and security of person and the right to be secure against unreasonable search and seizure). The Supreme Court as per McLachlin and LeBel found that the authorities executed a lawful search. Like the dissent, the majority stated that where information learned from a search could be used in an unfair trial, or to facilitate discrimination or political intimidation, or to commit human rights violations such as torture, then the sharing of information across borders would require additional measures to uphold the search such as Directives and caveats (see O’Connor Recommendations below). The court, however, stated that s 193(2)e of the Criminal Code (criminalises unauthorised interception of communications and disclosure of such information) did not permit disclosures that were inconsistent with ss 7 and 8 of the Charter. While the court upheld the constitutional validity of the information disclosure, they recommended that Parliament revisit s 193(2)e to provide more clarity and less ambiguity.

**R v Telus**

Telus is a communications company whose data practice is set up to store the content of text messages onto the company’s internal database for a period of time. This differs from

---

other telecommunications companies who do not store the contents of text messages, or if they do they store the contents for a brief time. The police out of Peel Station in Montreal used a general warrant as established in s 487.01 of the Criminal Code to obtain the contents of the stored texts of Telus customers.

There are many different types of warrants issued under s 487 of the Criminal Code. A general warrant has less barriers to obtain when compared with other types of warrants under s 487 including warrants to intercept private communications. In interpreting s 487(1)(c) Lebel, Fish and Abella JJ held that police are entitled to use a general warrant only where they can show that no other applicable provision that would allow an investigative technique. Other warrants, especially those involving new interception methods and those that may be more privacy invasive, typically require more specific and rigorous pre-authorisation requirements to obtain the warrant. The court further held that a technical interpretation of the work ‘intercept a private communication’ should not be used as this would effectively limit the scope of privacy protection when new communications technologies develop.

_R v Rogers_

Telecommunications companies Roger and Telus were given production orders by law enforcement to supply over 34,000 subscribers’ information with 200,000 records relating to at least 9000 individuals. These production orders were broad and onerous as they related to what is known as a ‘tower dump’ production order for all records of cellular traffic over a certain length of time. Such tower dumps include the name and address of every subscriber who made or attempted to communicate through a particular cellular tower. The production orders also require billing information which includes financial information such as banking details and credit card numbers. The companies applied to the court for a ruling that would make production orders more specific, and narrowly tailored to respect the privacy interests of their customers.

The Ontario Court of Appeal as per Sproat J. held that there is a reasonable expectation of privacy in the records; that Telus and Rogers have legal standing to assert the privacy interests of their subscribers; and that Production Orders infringe s 8 of the Canadian _Charter of Rights and Freedoms_. Justice Sproat went so far as to say, ‘I have no hesitation in finding that the Production Orders were overly broad and that they infringed s 8 of the Charter. The disclosure of personal information ... went far beyond what was reasonably necessary.’

The Court went one step further and offered specific guidance for law enforcement for future Production Orders. These were:

**Guidelines for Police**

[65] The police should include in the information to obtain a production order:

a) **One** – a statement or explanation that demonstrates that the officer seeking the production order is aware of the principles of incrementalism and minimal intrusion and has tailored the requested order with that in mind. An awareness of the Charter requirements is obviously essential to ensure that production orders are focused and Charter compliant.

b) **Two** – an explanation as to why all of the named locations or cell towers, and all of the requested dates and time parameters, are relevant to the investigation.

---

18 _R v Telus Communications Co_ [2013] 2 SCR 3, 76.
19 _R v Rogers Communications_ [2016] ONSC 70, 42.
This obviously flows from what is now the s 487.014(2)(b) Criminal Code requirement that there be reasonable grounds to believe that the documents or data requested will afford evidence respecting the commission of the offence.

c) Three – an explanation as to why all of the types of records sought are relevant.
   For example, the Production Orders sought bank and credit card information, and information as to name and location of the party to the telephone call or text communication who was not proximate to the robbery location. This information was clearly irrelevant to the police investigation.

d) Four – any other details or parameters which might permit the target of the production order to conduct a narrower search and produce fewer records.
   For example, if the evidence indicates that a robber made a series of calls lasting less than one minute this detail might permit the target of the order to narrow the search and reduce the number of records to be produced. If the evidence indicates that the robber only made telephone calls then there may be no grounds to request records of text messages. (Although the use of voice recognition software may make it difficult to distinguish between a person making a telephone call and a person dictating a text message.)

e) Five – a request for a report based on specified data instead of a request for the underlying data itself.
   For example, in this case a report on which telephone numbers utilized towers proximate to multiple robbery locations would contain identifying information concerning only a small number of robbery suspects and not the personal information of more than 40,000 subscribers which the Production Orders sought. This would avoid the concern expressed by Mr. Hutchison that 99.9% of vast amounts of tower dump personal information relates to individuals who are not actually suspects.

f) Six – If there is a request for the underlying data there should be a justification for that request.
   In other words, there should be an explanation why the underlying data is required and why a report based on that data will not suffice.

g) Seven – confirmation that the types and amounts of data that are requested can be meaningfully reviewed.
   If the previous guidelines have been followed the production order should be focused which will minimize the possibility of an order to produce unmanageable amounts of data. This confirmation does, however, provide an additional assurance.

Rogers is the latest case to assert that privacy rights will be upheld as technological advancements are made, and that the courts will require warrants or Production Orders, these must be appropriate, and must be narrow and tailored so as to avoid unnecessarily intruding on the privacy of those not subject to an investigation.

Summary and Implications

The courts have taken a strict view to interpreting lawful search and seizure when it involves an expectation of privacy, accessing or using data without a warrant in the context of an investigation, what types of warrants are appropriate for surveillance purposes, the validity of production orders, and whether there are appropriate controls around sharing data with foreign governments.
The Supreme Court has been firm and consistent where s 8 of the Charter is concerned. Lawful search and seizure requires an appropriate warrant if the information obtained is to be used in the course of an investigation leading to criminal charges. This is regardless if the information is obtained from an Internet Service Provider or a government agency.

Drawing inferences from data collected and used in Big Data systems in Canada will likely remain feasible for audit, and intelligence gathering, but the courts are drawing a clear line in the sand with respect for the requirements of appropriate warrants when using, interpreting and drawing inferences from data if they are to be used in any capacity to bring criminal charges.

Data analytics sometimes run using de-identified data. If a correlation is inferred from the data that there is the likelihood that for example a tax subject has committed tax fraud, is a warrant required for re-identification? Will new types of warrants be required to perform an intelligence scan to identify potential contraventions and those who have committed criminal acts? There are requirements around production orders for Telecommunications providers. Should production orders be extended to other sources of data collected by agencies and organisations other than Telecommunications Carriers? These decisions do not answer these questions. They do, however, indicate that the Supreme Court takes a very strong view about expectation of privacy, and that appropriate judicial authority will take into account the relevant technologies and practices of law enforcements agencies, as well as other agencies with the authority to investigate and apply criminal charges.

1.5 Reports and Frameworks

Like the United Kingdom and Australia, Canada has commissioned reports on privacy impacts of information sharing, reports in general about the intelligence community, and reports on national security and critical infrastructure. The most important of these are:

- **The Review of the Findings and Recommendations Arising from the Iacobucci and O’Connor Inquiries** (2009)
- **Office of the Privacy Commissioner of Canada, Special Report to Parliament – Checks and Controls: Reinforcing Privacy Protection and Oversight for the Canadian Intelligence Community in an Era of Cyber-Surveillance** (28 January 2014)
- **Security Intelligence Review Committee, Lifting the Shroud of Secrecy: Thirty Years of Security Intelligence Accountability** (2013–2014)
- **Auditor General of Canada, Protecting Canadian Critical Infrastructure Against Cyber Threats** (2012 Fall Report)

**The O’Connor Framework**

The Commission of Inquiry into the Actions of Canadian Officials in Relation to Maher Ara was led by Commissioner Justice O’Connor in 2006. Maher Ara was accused of aiding acts of terrorism and was handed over to United States authorities who sent him to be tortured in Syria for a year. A year later, Maher Ara was released and returned to Canada with a finding of him not having any ties to terrorists or terrorism. Justice O’Connor was appointed to lead a Commission of Inquiry into the incident. The result of this inquiry led to 23
Recommendations to restore public confidence in the police and the intelligence community. These recommendations listed below largely resemble some of the recommendations found in the 2015 RUSI report in the United Kingdom. Only those recommendations relevant to the use of data in relation with Big Data are considered. These have been shortened below:

Recommendation 6 – The RCMP should continue to share information with both domestic and foreign agencies but in accordance with the principles discussed in these recommendations.

Recommendation 7 – The Criminal Intelligence Directorate within the RCMP should have responsibility for oversight of information sharing with both domestic and foreign agencies.

Recommendation 8 – Mandatory screen for relevance, reliability and accuracy of information to be shared with other agencies in accordance with relevant laws respecting personal information and human rights.

Recommendation 9 – The RCMP should never share information in a national security investigation without written caveats in accordance with existing policy which places restrictions on who and how information may be used.

Recommendation 10 – The RCMP’s information-sharing practices and arrangements should be subject to review by an independent, arms-length review body.

Recommendation 11 – Canadian agencies that share information with the RCMP should review recommendations 6-10 to ensure that information sharing policies are consistent with these principles.

The above recommendations are concerned with similar principles found in the Lens such as proportionality, accountability, reliability and integrity of data, and respect of privacy and human rights. These recommendations are aligned with the human rights and freedoms protected under the Canadian Charter of Human Rights and Freedoms. Much legislation and policy directives, as we will see in Chapter 3, incorporates many principles found not only in the Charter but in the O’Connor Recommendations. As the case law highlights, the Canadian courts protect privacy and human rights in Charter litigation, and any use of Big Data systems that leads to investigations and criminal charges will attract scrutiny.

Although the Treasury Board sets relevant policies and frameworks relative to Big Data, intelligence agencies are not strictly bound to follow these policies and frameworks. This will be explored further in Chapter 3.


2. USING BIG DATA FOR NATIONAL SECURITY: STAKEHOLDERS’ PERSPECTIVES

The goal of this chapter is to capture understandings, perceptions and views of individual research participants on a range of issues. It is important to emphasise that the empirical findings presented in this chapter provide a snapshot of the views and perceptions of research participants only. These views and perceptions may or may not be based on a comprehensive or accurate understanding of the issues involved. Given that the sample size is relatively small and not necessarily representative of the population of stakeholders in Canada, the findings are meant to indicate issues and not to be read as a comprehensive coverage of all relevant information. We do not attempt here to evaluate or correct research participants’ views, although we have included cross-references to other sections in the report where appropriate.

Terminology used to describe categories of research participants is contained in Chapter 4 of the Methodology Report. 22

Those interested in the conclusions drawn from interviews, as well as the broader trends across interviews, may choose to focus on the ‘Summary and Implication’ boxes rather than the extended quotations from particular interviews. Letters are used to mark quotations from interviews for cross-referencing purposes.

2.1 Current Use of Data

2.1.1 General attitudes towards computer technology

We asked research participants who were working in or had worked in operational organisations, ‘When does digital/computer technology hinder you in your work and when is it particularly helpful?’ [O3] The question is designed to elicit immediate reaction to digital technology in general before discussing specifics in relation to the use of data.

Table 2-1 General Attitudes towards Computer Technology (n=6)

<table>
<thead>
<tr>
<th>Attitude</th>
<th>TOTAL (n=6)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Both helpful and a hindrance</td>
<td>2</td>
</tr>
<tr>
<td>Helpful</td>
<td>0</td>
</tr>
<tr>
<td>A hindrance</td>
<td>1</td>
</tr>
<tr>
<td>No responses recorded or question not asked</td>
<td>3</td>
</tr>
</tbody>
</table>

22 The abbreviations are: O for Operational, T for Technical and P for Policy, with O/O for example representing a research participant with an operational role working in an operational organisation. It is crucial to note when reading this chapter that, in accordance with our project methodology we interviewed 11 people in Canada who were or are working in operational (6), policy (1) independent (2) or research non-government (2) organisations. We did not interview anyone working in technical organisation, as many of these are related companies of those interviewed in Australia. In Australia, we relied heavily on CRC partners to nominate people within their own organisations. For Canada we relied on diplomatic assistance as well as local professional and personal contacts. Differences in recruitment methods, fieldwork time frame, and individual willingness to participate mean that the sample of interviewees in Canada may not be directly comparable to the Australian one. In particular, three of the six research participants in operational organisations in Canada worked in technical roles. Additionally, there were four research participants out of eleven who, while they no longer worked for operational organisations, used to work for various intelligence agencies in Canada and abroad. In each of these cases, the research participant was asked to comment on questions from multiple perspectives if they wished to do so.
*Note: Only those working in or had worked in operational organisations are asked this question.

**Summary and Implications**

While technology was considered helpful it was also seen as a hindrance, in particular where the technologies used were considered out-dated and insufficient for the organisation’s needs.

### 2.1.2 Types of data used

Types of data used were substantially similar to Australia for Operational, Technical and Policy. Table 2-2 below breaks down the types of data used. Note that there were only three responses — although six research participants came from operational organisations, only three of the six answered the questions around operations. The other three answered the technical questions which did not include the question ‘what type of data does your organisation use’. Of the three research participants who answered the operational questions, we did not have representation from certain intelligence agencies. For example, we have only one organisation stating that they use telecommunications data when this is clearly not the case as will be further seen in Chapter 3.

**Table 2-2: Type of Data Used (n=3)**

<table>
<thead>
<tr>
<th>Type of Data</th>
<th>TOTAL (n=6)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Open source/online data</td>
<td>1</td>
</tr>
<tr>
<td>Telecommunications metadata</td>
<td>1</td>
</tr>
<tr>
<td>Intelligence data</td>
<td>2</td>
</tr>
<tr>
<td>Communication signals</td>
<td>1</td>
</tr>
<tr>
<td>Any data we have legal access to/numerous datasets</td>
<td>1</td>
</tr>
<tr>
<td>Operational /official data /data from other government departments</td>
<td>3</td>
</tr>
<tr>
<td>Data from international partners</td>
<td>1</td>
</tr>
<tr>
<td>Publicly available data</td>
<td>2</td>
</tr>
<tr>
<td>Databases internal to the agency</td>
<td>3</td>
</tr>
<tr>
<td>Information provided by the community</td>
<td>1</td>
</tr>
<tr>
<td>Geo-spatial data</td>
<td>1</td>
</tr>
<tr>
<td>Financial data</td>
<td>1</td>
</tr>
<tr>
<td>Investigative data</td>
<td>2</td>
</tr>
<tr>
<td>Raw data</td>
<td>2</td>
</tr>
<tr>
<td>Unstructured data</td>
<td>2</td>
</tr>
<tr>
<td>Summarised Reports</td>
<td>3</td>
</tr>
<tr>
<td>Incident statistics</td>
<td>2</td>
</tr>
<tr>
<td>Performance information and management data</td>
<td>2</td>
</tr>
</tbody>
</table>

*Note: Multiple responses can be coded for each research participant. Only those working in or had worked in operational organisations are asked this question.

### 2.1.3 Types of data generated

This question was deliberated omitted from the Canada study.
2.1.4 Sharing of data

We asked research participants who were working or had worked in operational organisations ‘Does your agency/unit share data with other agencies and, if so, which ones?’ [OS] and ‘What kind of data is shared – is it raw or summarised; identified or de-identified?’ [O6]. Data sharing appears to have some differences in Canada when compared with Australia as will be discussed below. Table 2-3 provides a general picture of who shares data with whom. This information was based on only three research participants as noted in the last section.

Table 2-3: Sharing of Data between Canadian Organisations

<table>
<thead>
<tr>
<th>Canadian national security organisations</th>
<th>Canadian law enforcement organisations</th>
<th>Other Canadian government organisations</th>
<th>Civil society, media, community</th>
<th>International organisations</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Intelligence community</td>
<td>• Summarised Reports</td>
<td>• Defence Research development Canada</td>
<td>• Not identified in the interviews.</td>
<td>• Five Eyes community</td>
</tr>
<tr>
<td>• Treasury Board</td>
<td>• RCPM</td>
<td>• Government operations centre</td>
<td></td>
<td>• Other countries require special authorisation with caveats based on the O’Connor Recommendations that were discussed in Chapter 1</td>
</tr>
<tr>
<td>• Case by case basis but could include all departments &amp; organisations identified in SCISA legislation</td>
<td>• Ottawa police</td>
<td>• Operation Intersect</td>
<td></td>
<td>• 24/7 Network contact from participating countries in the Convention on Cybercrime</td>
</tr>
<tr>
<td>(See Table 1-1 for SCISA entities)</td>
<td></td>
<td></td>
<td></td>
<td>• Interpol, Europol</td>
</tr>
<tr>
<td>Canadian law enforcement organisations</td>
<td>• Intelligence community</td>
<td>• Social Services</td>
<td>• Media</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Health Canada</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>• All Departments and organisations identified in SCISA legislation</td>
<td>• Citizens (FOI)</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>• (See Table 1-1 for SCISA entities)</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Provincial and municipal police forces</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Other Federal or Provincial investigative agencies</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Canada Customs and Immigration</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Source: Interview participants working in or had worked in operational organisations.

A few common themes about data sharing emerged from the interviews:

Inter-agency sharing within Canada

The default regime in Canada is that you can share data between governmental agencies and non-governmental organisations provided there is not an express provision or rule stating otherwise. Some research participants stated:

We don’t know what C51 will do or how it will affect us. It does not get you around any explicit prohibitions on sharing. You can share (with Canadian agencies) unless you are not explicitly allowed to share. (O-T/O A)

On a national level we share with everyone where necessary. The sharing is case specific to meet department mandates and increasingly with the broader security community under SCISA which is part of Bill C51. Under SCISA there’s a very broad
definition of the security community so we would share with Health Canada, and the CRA for example. (O/O B)

Sharing with foreign agencies

Sharing of data between Canadian and foreign agencies appears to elicit more concerns and there are more constraints around information sharing. As stated below from research participants from operational organisations regarding sharing:

... internationally – almost always case specific and with Europol, Interpol and Five Eyes with rare exceptions but vast majority of time on case-by-case circumstance-specific based on principles of proportionality and relevance, reliability and accuracy – the O’Connor Principles set the framework. (O/O C)

... sharing – once burned twice shy. The O’Connor Recommendations are the cornerstone of sharing, and need to know, proportionality, necessity as they resemble the Charter as well as consistent use with s 8 of the Privacy Act. My worry is that over time as we deal with increasing amounts of data our ability to have constraint will lessen with how we share data. (O-T/O D)

The last sentiment is interesting as the research participant believed that Big Data wouldn’t lead to greater sharing between foreign agencies but the reverse, where there would be more constraints imposed around sharing information with foreign agencies, but less ability to have meaningful constraints.

Over-classification of data restricts sharing

Two participants (O) identified a culture of over-classification creating problems of sharing classified data between government agencies and stakeholders. One research participant stated:

There is a trend of over-classification where people take more precaution than necessary. (O/O E)

The research participants did not identify whether classified documents were concerned with secrecy, sensitive information or other. Another research participant noted:

[there is a] real problem with access between government and stakeholders. For example, working with various private companies … the government might ask an airport to raise your fences around the airport with barbed wire but who is going to pay? Why do we need to raise our fences and spend millions? Oh, I cannot tell you … The Integrated Terrorism Assessment Centre shares assessments of the threat with government and stakeholders and they used to ask stakeholders to use unclassified products. Now the question is, if not enough information has been communicated then you can’t convince private corporations to do what you ask of them without them wondering why you have to do this. So you’re dealing with people who ‘have a need to know why they need to do something’ but don’t have ‘state clearance’ in order to be a party to the ‘why’. In the U.S. they do more work around these issues with fusion centres all across the country. (O-T/O F)

The above research participant suggested that sharing classified information (and even unclassified information as seen in the above quote) between the government and private corporations could be improved. The quote further identifies Canada as an Integrated Terrorism Assessment Centre whose role it is to share threat assessments with government and private stakeholders but it is seen as requiring improvement. This participant also indicated that the Canadian ITAC is staffed with former intelligence officers who do not know how to communicate with the private industry, whereas there were many similar
‘fusion’ centres in the United States to fill this role and they were staffed with people with good communications skills.

Summary and Implications

<table>
<thead>
<tr>
<th>There is sharing of data between agencies domestically and internationally with different rules applying to different contexts. Users identified that the default rule in Canada is that sharing between domestic agencies is allowed unless expressly prohibited. In the international context it was more complicated. Users pointed out that there had been problems with sharing in the past leading to Charter of Human Rights violations including torture. Data sharing among agencies and with foreign counterparts involves decisions that are not easily automated. This led to the so-called O’Connor Recommendations discussed in Chapter 1 and as identified in the interviews.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Sharing information occurred between government organisations (law enforcement, other related to national security), non-government organisations, and between foreign agencies. The extent of sharing was not identified in the interviews. The participants also identified three aspects that did not arise in the Australian context. These were: over-classification of data preventing sharing; there are few impediments to sharing information between Canadian agencies; and that there were concerns raised with regards to sharing information with foreign agencies.</td>
</tr>
</tbody>
</table>

2.1.5 Main purpose of using data

All six participants from operational organisations were asked: ‘What do you (or your unit) mainly use these data for?’ [O10] Canadian research participants identified several purposes for the use of data. There are:

- Investigations inclusive of national security investigations
- Disruption
- Intelligence collection for future analysis
- Business intelligence
- Managing programs
- Efficiency metrics
- Administration and security investigations
- Trend prediction
- Emerging best practices
- To pass on intelligence to the appropriate decision-making entity

There were some different data uses mentioned in the Australian interviews. Only one research participant noted that they were using Big Data to manage their employees, and sell to third parties as a source of revenue. (T-O/O G) Another research participant noted that the Government needed to start to use data as its foremost asset noting:

We need to transition a data asset from something being owned by one program of infrastructure to become an asset of the government as a whole... Information is the only asset the government has. (T-O/O H)
**Summary and Implications**

The three Canadian research participants from operational organisations emphasised the importance of using data not only to identify trends but to enable better business management. As in the Australian study, there were also diverse responses including predicting trends, disruption, intelligence for investigations, business intelligence and efficiency metrics.

2.2 **Current concerns regarding access to and sharing of data**

Participants from operational organisations were asked, ‘What are your major concerns in relation to data access from other agencies or sharing data with other agencies?’ [07] Table 2-4 summarises the responses to this question, broken down by the role of research participants in their respective organisations. A number of concerns were raised: legal requirements including legal or privacy issues (real or perceived), technical issues, and other issues related to ownership and trust, requirements and safeguards for data sharing, and lack of capacity to process data.

**Table 2-4: Current Concerns re Access to and Sharing of Data by Role in Organisations (n=6)**

<table>
<thead>
<tr>
<th>Concern</th>
<th>O/O (n=3)</th>
<th>T/O (n=2)</th>
<th>O-T-P/O (n=1)</th>
<th>TOTAL (n=6)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Legal requirements/privacy – real or perceived</td>
<td>3</td>
<td>1</td>
<td>1</td>
<td>5</td>
</tr>
<tr>
<td>Technical issues</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>3</td>
</tr>
<tr>
<td>Ownership and trust</td>
<td>1</td>
<td>1</td>
<td></td>
<td>2</td>
</tr>
<tr>
<td>Uncertainty of requirements around sharing and Sharing with inadequate safeguards</td>
<td>2</td>
<td></td>
<td>1</td>
<td>3</td>
</tr>
<tr>
<td>Lack of capacity to process data</td>
<td>1</td>
<td></td>
<td>1</td>
<td>2</td>
</tr>
</tbody>
</table>

*Note: Multiple responses can be coded for each research participant. Only those working in or had worked in operational organisations are asked this question. One research participant wasn’t asked this question.*

2.2.1 **Real or perceived legal requirements**

Research participants identified privacy or legal requirements as something to be overcome for access and sharing.

Their concerns featured prominently on insufficient control around access to data and databases coupled with insufficient oversight. One research participants noted:

> Data access and sharing with other agencies generates concerns ... We don’t know what Bill C51 will do or how it will affect us.... (O/O I)

Another research participant noted that the sharing rules were not problematic between government agencies but more between government and stakeholders:

> Are the rules (around access and sharing) adequate? I think they are. C51 will aid this. The real problem with access and sharing is between government and stakeholders. (O-T/O J)

Uncertainty of requirements around sharing, and the inadequacy of sharing safeguards was mentioned by the majority of research participants from operational organisations.

One research participant who used to work in a senior position in operations went so far as to say that for Canadian intelligence agencies there was a ‘worrying trend allowing security
intelligence to operate in violation of the Charter ... in terms of internal barriers [for access, sharing], there are none.’ (P-O/P K).

2.2.2 Technical issues

Five out of the six research participants from operational organisations spoke about technical issues. Research participants spoke of the problem of stand-alone web systems and legacy systems that are incompatible between agencies as well as out-dated technologies not up to the challenges organisations are up against. One participant from an operational organisation noted that there were even interface integration problems within the same organisation with the use of not one but two different systems with the same data. (T-O/O L)

2.2.3 Data ownership and trust

Trust issues and data ownership were a recurring theme in both the Australian and Canadian interviews.

Data ownership, however, was less of a concern in the views of the Canadian research participants compared to trust issues. In the Canadian interviews trust came up in several different ways explored below.

**Person-to-person**

Research participants expressed that they didn’t know yet how Bill C-51 would change sharing amongst agencies and indicated that under the former government sharing was not done agency to agency, but, rather from trusted person to trusted person within agencies, as one participant indicated:

That trust was done person to person in this Federal government under Prime Minister Harper and the Conservative Party. They are very trust based and person based, so contact to contact and less agency to agency. (O/O M)

**Too much trust in other nations**

The second way in which trust was distinguished from the Australian interviews had to do with the O’Connor Commission and Recommendations where research participants acknowledged the mistakes made in the Maher Ara incident of an innocent man being tortured for close to a year before being sent back to Canada from an American camp in Syria. Put differently, there was an expression of less trust between Canada and the United States, than with Canada and the United Kingdom, New Zealand and Australia. One research participant stated:

... my greater concern with allies (the United States) is that they don’t play by those rules and US Patriot Act is a significant impediment and concern. This is less with Australia and the UK and New Zealand. (O/O N)

The research participants consistently stated that sharing of data with foreign nations does not occur in a broad manner such as sharing real-time feeds to raw data. Summarised reports are shared, and more specific data is shared on a case-by-case basis with the United States due to lack of control over what is done with the data/information.
Summary and Implications

As in Australia, legal requirements were the primary concern among research participants from operational organisations. While privacy controls were mentioned by participants from both countries, technical issues, and ownership and trust issues were also important factors in the Canadian responses. Issues around sharing data and lack of capacity to process data were seen as important and unresolved issues from the Canadian responses including how trusts has previously been done person to person, and how there were growing concerns around the lack of sharing controls with foreign agencies.

Three main concerns were raised, however, legal requirements made up the majority of concerns among research participants. While privacy controls were mentioned from research participants from both Canada and Australia, sharing control issues and ownership/trust issues were important factors in the Canadian responses. Technical issues were also present in Canada.

Legal requirements: The most frequently cited concern related to real or perceived legal requirements, including relation to sharing and privacy issues. Participants readily referred to the information sharing aspects of the new piece of legislation known as Bill C-51.

Technical issues: These related mainly to matters such as data format, data ‘silos’, non-availability of historical data, the agency’s ability to deal with the volume of data, and the continued use of legacy technology.

Data ownership and trust between agencies or individuals were the two factors that appear to explain some of the reluctance to share data. Reference was made to cultural issues (reluctance to trust the quality of data from another agency; legal responsibility for use of data; and general control issues) that make data sharing challenging.

2.3 How problems can be overcome

We asked the same operational research participants ‘How can these problems be overcome?’ [O9] Table 2-5 provides responses broken down by the current concerns expression in the previous section. The number of participants who expressed concerns in table 6 is provided in ( ) below the type of concern.

Table 2-5: Current Concerns by How Problems Can Be Overcome (n=6)

<table>
<thead>
<tr>
<th>Legal requirements/privacy</th>
<th>Technical Issues</th>
<th>Ownership and trust</th>
<th>Sharing</th>
<th>Capacity to Process</th>
</tr>
</thead>
<tbody>
<tr>
<td>Law reform/guidelines/policy decision</td>
<td>(5)</td>
<td>(3)</td>
<td>(2)</td>
<td>(2)</td>
</tr>
<tr>
<td>Education/training of practitioners</td>
<td></td>
<td>1</td>
<td>1</td>
<td></td>
</tr>
<tr>
<td>Better data management</td>
<td></td>
<td></td>
<td></td>
<td>1</td>
</tr>
<tr>
<td>Conversation with public</td>
<td>1</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Cultural change</td>
<td></td>
<td>1</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>Political environment</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

* Note: Multiple responses can be coded for each research participant. The number in brackets in the first row represents the number of research participants who raised that issue, see Table 2-4. Only those working or had worked in operational organisations are asked this question. Only two participants responded to this question out of 6 who discussed concerns in Table 6.
As only two research participants answered the question it is difficult to draw inferences from their responses. However, there were answers from the entire pool of research participants which highlighted possible solutions to the problems articulated in 2.2. This is because three of the other research participants used to have roles in operations, or currently work for operations but elected to answer a different set of questions (two participants). Their expertise, experience and comments in the interviews are, therefore, relevant to this section.

2.3.1 Legal requirements or privacy issues

Although the research participants identified some legal and privacy issues, there were only a few responses addressing how access problems could be overcome.

One research participant thought that risks, privacy or otherwise, could be best managed if the government treated all data the same, and had a federated system with controls around access and use similar to what banks provide including constant backups, early warning systems, 24 hour monitoring, and reviews. (O-T-P/O O)

2.3.2 Technical Issues

Technical limitations were expressed in answering questions around concerns and problems with 3/5 indicating these were concerns. Other participants offered opinions about technical issues during the course of the interview, but not necessarily in response to questions O8 and O9. In the Canadian interviews across operational and policy organisations a spectrum of technical issues were raised. As one person put it,

"Our ability to write warrants to get information exists but the ability to process that information isn’t there. (O/O P)"

Standardisation of technologies and protocols in different agencies coupled with a limited cultural uptake of the technology, posed a significant issue for current data systems, as well as for future Big Data systems. This response was similar in Australia and Canada with one notable difference – the Canadian participants identified that Canada lacked Big Data capabilities in spite of the ability to share data and information across agencies. (T-O/O)(O-P/P)(O/O).

Legacy systems require a large investment across most Canadian agencies to allow for the advantages and benefits that Big Data may bring. It was noted that sharing between intelligence agencies amongst the Five Eyes had no identified technical impediments, but sharing intelligence or data between Canadian agencies was significantly more limited. As stated by one research participant:

"Sharing amongst national agencies (is a) more limited in capacity (where agencies have) secure stand-alone web based databases for each agency ... which do not allow for sharing of raw data. (O-T/O Q)"

In a manner similar to Australia, summarised reports were mostly shared between agencies. Raw data was less frequently shared less while most data was identifiable as de-identification techniques were not used.

One technologist thought that while there were many advantages to Big Data analytics, there were no advantages to use of bulk datasets in the context of national security because they create too many false positives, and would slow down an investigation. The potential technical solution was to combine bulk telecommunications metadata sets with content such as emails as this is the only way to produce less false datasets, and better explain correlations. AMC24 (O-T/O)
2.3.3 Ownership and trust

One research participant who had extensive experience in technology systems, operations of the intelligence sector, and policy experience with multiple federal agencies identified data ownership as the single most difficult problem to solve culturally. When asked how he/she or his/her organisation would improve systems the answer was unique:

... make all data records with the same definition of ‘record’ in all Acts... We need to transition a data asset from something being owned by one program or infrastructure to become an asset of the government as a whole... the only asset the government has is information. A centralised system requires federated access like Star Trek. You can manufacture a centralised repository and solution framework for unstructured data for an enterprise solution. Metadata would be standardised and attached automatically and contained in a centralised repository and that access can be permissions based. Institutions could still find their own holding within that centralised base ... You’re not dealing with what to put in the system. Everything is in the system. (T-O/O R)

The above statement is interesting from a comparative perspective. The ACC’s new role and centralised database structure in many ways is an example of the above with the difference that in the Canadian research participant’s opinion, all data should be in the centralised system and not just data used to solve crimes.

2.3.4 Cultural

Cultural challenges were seen as being a major obstacle to successfully overcoming concerns about data access, usage and sharing. A research participant noted:

I would say that the easy answer is technology but it’s not the right answer because the near as I can tell the best way to do it is will. It’s the only thing that conquers it and fundamentally plays with the heart of policing. The policing attitude is if you don’t have a system that works exactly how I need it I will do it myself. We also have a failure of imagination from the 55 year old men stereotypes making the decisions in policing. They don’t use technology or data when making decisions about technology. These are all institutional failures. (O/O S)

Another research participant described the problem in the national security space, there is a ‘culture of secrecy and over-protection’ (O-P/P T) which needed to change in order to provide solutions to the various problems with the use of data in law enforcement and intelligence.

2.3.5 General

Sufficient resources were seen as a requirement for existing and future data systems and technologies to succeed. Insufficient number of staff and insufficiently trained staff remain problems which may be overcome. Interestingly, the ability to overcome staffing problems was identified by at least one to have very little to do with recruiting those with intelligence experience; the problem it would seem is that people with intelligence experience are often hired to work as managers and key communicators but have little training to succeed at their mission. (T-O/O U)
Summary and Implications

While only two research participants directly answered the question how can problems be overcome, there were points in the interviews when discussing other concerns and risks where resolving problems was identified. The two participants both identified cultural change as important in addressing concerns including change in sharing, ownership and trust, as well as resolving technical concerns. Other inferences drawn generally from the other interviews included resolutions to concerns through providing sufficient resources both for the staff and for acquisition of technologies.

2.4 Big Data: potentials, limits and risks

2.4.1 What is Big Data?

Interestingly none of the research participants gave us a definition of Big Data stemming from a government framework, document or guideline. There is no accepted definition or standards of Big Data in Canada and within the Canadian government. There were two interviews where the question wasn’t directly answered. Definitions provided were substantially similar to those research participants in Australia and the United Kingdom.

Table 8 provides a list of the main responses from research participants to the question: ‘How would you define Big Data?’ [O13, T3, P3] broken down by their role and the type of organisation they worked in. The most frequently mentioned attribute of Big Data was in terms of volume (10/11), its analytic prediction (8/11), followed by aggregation/integration (7/11). As seen in the table, there were a few people in each of the remaining categories. Volume was often mentioned together with some predictive or analytics capacity, and the ability to aggregate data.

Table 2-6: Conception of Big Data by Role and Type of Organisation (n=11)

<table>
<thead>
<tr>
<th></th>
<th>O/O (3)</th>
<th>T/O and T-O/O (2)</th>
<th>O-T-P/O (1)</th>
<th>O-P/P and P/P (5)</th>
<th>TOTAL (11)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Volume</td>
<td>3</td>
<td>2</td>
<td>1</td>
<td>4</td>
<td>10</td>
</tr>
<tr>
<td>Analytic/ prediction/ unlocking hidden results</td>
<td>2</td>
<td>1</td>
<td>5</td>
<td>8</td>
<td></td>
</tr>
<tr>
<td>Aggregated/ integrated data</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>4</td>
<td>7</td>
</tr>
<tr>
<td>Beyond human &amp; established technology</td>
<td>2</td>
<td>1</td>
<td>1</td>
<td>4</td>
<td>7</td>
</tr>
<tr>
<td>Variety</td>
<td>1</td>
<td>1</td>
<td>2</td>
<td>4</td>
<td>4</td>
</tr>
<tr>
<td>Velocity</td>
<td>1</td>
<td>1</td>
<td></td>
<td>2</td>
<td>2</td>
</tr>
<tr>
<td>Marketing</td>
<td></td>
<td>1</td>
<td>1</td>
<td>2</td>
<td>2</td>
</tr>
</tbody>
</table>

*Note: Multiple responses can be coded for each research participant.

Summary and Implications

‘Big Data’ is a term without a single precise meaning; rather it is used to articulate a range of practices. In the context of national security and law enforcement, research participants’ definitions of Big Data were focussed on both technical and user requirements. The main requirements relate to handling volume, analytic capacity to provide useful and reliable information, and dataset integration.
Definitions of Big Data had similar attributes with responses from the Australian Study. Veracity, however, was not mentioned by any of the Canadian research participants.

2.4.2 Capability of Big Data

Research participants’ identified many different Big Data capabilities. The question was framed so that research participants were asked, ‘what is Big Data capable of doing that ‘ordinary data’ can’t?’ Unlike the Australian and UK research participants working for an Operations organisation, three Canadian participants elected to answer the technical questions. The technical questions did not query capabilities of Big Data. The shaded rows are responses not found in the Australian or UK Reports. Table 2-7 below breaks the responses down further.

Table 2-7: Perceived Capability of Big Data by Role and Type of Organisation (n=8)

<table>
<thead>
<tr>
<th>Capability</th>
<th>Operational (n=3)</th>
<th>Policy (n=5)</th>
<th>TOTAL (n=8)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Analytic capability</td>
<td>1</td>
<td>5</td>
<td>6</td>
</tr>
<tr>
<td>Opportunity for discovery of unforeseen insights and categories</td>
<td></td>
<td>5</td>
<td>5</td>
</tr>
<tr>
<td>Identification of patterns and trends</td>
<td>1</td>
<td>4</td>
<td>5</td>
</tr>
<tr>
<td>Need caution re expectations</td>
<td>1</td>
<td>2</td>
<td>3</td>
</tr>
<tr>
<td>Richness of data</td>
<td>1</td>
<td>1</td>
<td>2</td>
</tr>
<tr>
<td>More data driven decision-making</td>
<td>1</td>
<td>1</td>
<td>2</td>
</tr>
<tr>
<td>Improved efficiency/effectiveness</td>
<td></td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>Risk management</td>
<td>1</td>
<td></td>
<td>1</td>
</tr>
<tr>
<td>Drawing Correlations</td>
<td>1</td>
<td></td>
<td>1</td>
</tr>
<tr>
<td>Ability to test and retest hypotheses</td>
<td></td>
<td></td>
<td>1</td>
</tr>
</tbody>
</table>

*Note: Multiple responses can be coded for each research participant.

The research participants identified a range of capabilities for Big Data. The responses focused heavily on trend prediction and futuristic abilities. These were data analytics (6), patterns and trends (5) and discovering unforeseen insights (5). Two new categories were identified: drawing correlations and the ability to test and retest hypotheses (note that there was only one participant for each of these categories). Four out of 8 thought ‘identification patterns and trends’ was one of Big Data’s capabilities but 3 expressed the view that caution around expectations is required.

Identification of patterns and trends

Several research participants highlighted that identification of patterns/trends and predictive capabilities would be the greatest capability and benefit.

Three research participants in operations and policy were doubtful of its utility as they thought that the expectations around Big Data required caution. As some of the research participants noted:

- Big Data has the capacity to make big mistakes. The data led us here so this must be right. (P/P V)

- With Big Data you can draw solid correlations but not establish cause effect relations ... but you have to be careful what you conclude from that. (O/O W)
Risk management

One research participant stated:

I think it allows you to look at the big picture, trends (black swans) so that you can better manage risks and not be reactionary, and more difficult to manage and position controls and plans to prevent the risk and reduce their impacts. (O/O X)

Improved efficiency/effectiveness

Additionally one of the research participants saw data analytics whether Big data or other, to present ways for an organisation to better manage its resources leading to gains in efficiencies. (T-O/O Y)

Summary and Implications

In terms of capability, Big Data was seen by research participants as involving analytic capacity, ‘rich’ data, the ability to identify patterns and trends, improved efficiency and effectiveness, and enabling data-driven decision making. Not every participant saw an advantage to Big Data, and three cautioned against unrealistic expectations while two believed that governments would be very slow to uptake Big Data, and even slower to do so in a cost effective way. They thought that a lack of culture and training could make Big Data less relevant as decision-makers were more likely to have traditional social science backgrounds and may not understand the how big data methodologies differ.

<table>
<thead>
<tr>
<th></th>
<th>Operational (6)</th>
<th>Policy (5)</th>
<th>TOTAL (11)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Yes (including “to some extent”)</td>
<td>3</td>
<td></td>
<td>3</td>
</tr>
<tr>
<td>Yes but varies</td>
<td>2</td>
<td>2</td>
<td>4</td>
</tr>
<tr>
<td>Perceived yes</td>
<td></td>
<td>3</td>
<td>3</td>
</tr>
<tr>
<td>No</td>
<td>1</td>
<td></td>
<td>1</td>
</tr>
</tbody>
</table>

Note: Frequencies in cells do not represent number of agencies, as there were multiple research participants from some agencies.

Only three participants in operational organisations claimed to be using Big Data in their work (O/O)(T/O). One of these organisations uses Big Data for research purposes which later feeds back to the appropriate government agency. One participant implied that Big Data was used for risk management purposes to drive the business case (T-O/O). While one operational organisation stated that they used data and data analytics, but they do not currently use Big Data.

Four of the research participants (2 from policy and 2 from operational organisations) had previous experience working for intelligence agencies in Canada, the United States and the United Kingdom where they all expressed that more advanced Big Data analytics were being used but whether or not they were being used well with tangible benefits seemed to be an open ended question amongst those interviewed, or at least in the Canadian intelligence space.

By contrast some research participants were clear that they thought larger private organisations in Canada were using Big Data systems such as Canada Post, Bell and Google.
These organisations were identified as using Big Data in a variety of ways including employee management, services delivery, and for third party sale as a source of revenue.

Summary and Implications

Only three participants in operational organisations stated that they were using Big Data, while the other participants stated that they were just starting to use Big Data visualisation tools, but the uptake had so far been slow. This may suggest that their conceptions of Big Data and its capability and value were not necessarily based on first-hand knowledge or experience with this technology, however, two of these participants worked with Big Data on a daily basis and one programmed bespoke tools used within their organisation.

The small sample size makes it difficult to identify trends. No one indicated that they were using bulk data-sets but two participants stated clearly that they were using Big Data analytics (whether an organisation used bulk datasets was not directly asked).

2.4.4 Current use of data analysis tools

While most of the participants from operational organisations reported that their agency used some form of data analysis, the analysis was limited to more traditional social sciences methodologies, and data mining was not regarded as Big Data under their definitions. Some of the participants said that more sophisticated data analytics was certainly on the horizon for their organisation.

Table 2-9: Current Use of Data Analysis Tools by those in Operational Organisations (n=6)

<table>
<thead>
<tr>
<th>Data Analysis (in general)</th>
<th>Number of participants (6)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Off the shelf tools</td>
<td>3</td>
</tr>
<tr>
<td>Custom tools</td>
<td>3</td>
</tr>
<tr>
<td>Data visualisation/Mapping</td>
<td>3</td>
</tr>
<tr>
<td>Statistical analysis</td>
<td>1</td>
</tr>
</tbody>
</table>
| Data browsing/ searching/ sorting/ linking/ summarising | 1

* Note: Multiple responses can be coded for each research participant. Only those representing operational organisations are included in this table.

Summary and Implications

Most participants from operational organisations indicated that they have been using data analytics and statistical analysis for quite some time, but the use of machine learning or predictive tools was not mentioned. As in Australia organisations were using both off the shelf and custom tools.

2.4.5 Barriers and challenges to using Big Data

On the whole the research participants identified more barriers and challenges to using Big Data than they did benefits. Some of the barriers identified could be removed with some effort while others would require more serious changes.

There is a lack of understanding around why and how to use Big Data. This was expressed well by one research participant:
...we have information, personal information banks, and departments have to disclose what we’re collecting e.g. Business Continuity Plans, then we have to say to the public we are collecting this information for that reason but that isn’t how Big Data works. You don’t collect the information for any particular reason. (T-O/O Z)

Table 2-10 below breaks the barriers and challenges down further.

Table 2-10: Barriers/Challenges to use of Big Data by Type of Organisation (n=11)

<table>
<thead>
<tr>
<th>Barriers/Challenges</th>
<th>Operational (6)</th>
<th>Policy (5)</th>
<th>TOTAL (11)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Legal/privacy issues (including consent, requirements, proportionality)</td>
<td>5</td>
<td>3</td>
<td>8</td>
</tr>
<tr>
<td>Cultural Issues</td>
<td>3</td>
<td>3</td>
<td>6</td>
</tr>
<tr>
<td>Access to Sharing of Data/Data Silos</td>
<td>2</td>
<td>1</td>
<td>3</td>
</tr>
<tr>
<td>Technical and other resources</td>
<td>2</td>
<td></td>
<td>2</td>
</tr>
<tr>
<td>Accountability</td>
<td>2</td>
<td></td>
<td>2</td>
</tr>
<tr>
<td>Public acceptance/trust</td>
<td>0</td>
<td>2</td>
<td>2</td>
</tr>
<tr>
<td>Data format/data quality/no standard</td>
<td>1</td>
<td>0</td>
<td>1</td>
</tr>
<tr>
<td>Distrust of data within organisation</td>
<td>0</td>
<td>1</td>
<td>1</td>
</tr>
</tbody>
</table>

Note: Multiple responses can be coded for each research participant

While eight participants identified legal issues, seven participants identified privacy issues in particular as a barrier to the use of Big Data. As will be seen in Chapter 3, legal requirements around privacy do not present a significant barrier. This may suggest that there is a culture of acknowledging privacy issues and a lack of sharing between agencies (silos) regardless of what is permissible by law. Cultural issues were a barrier in Australia as well. In Canada technical and resource issues were also a problem.

Summary and Implications

Barriers to the use of Big Data on the whole were similar in Canada to those in Australia. Legal requirements were presented as a challenge to Big Data. Ironically it was a lack of adequate privacy laws that was perceived as the barrier; not that privacy laws prevented Big Data usage. Some research participants discussed how the Privacy Act was out of date and unsuited to technologies in general generating a hesitancy and reluctance to move toward more invasive technologies, and that the Act contained much weaker provisions than PIPEDA which governs private organisations.

Research participants identified cultural and technical barriers as a significant challenge. There were a variety of cultural barriers to greater use of Big Data for law enforcement and national security. These include the fact that Big Data is unlikely to be used unless there is institutional support and appropriate levels of trust, and confidence in technology among users.

2.4.6 Risks of Using Big Data

To examine participants’ perception of the risks of using Big Data, we asked a similar question of each group: ‘What are the risks of using Big Data for law enforcement or security intelligence?’ [O19 and P10]. Risks identified by participants are broken down in Table 2-11.
Table 2-11: Risks of Using Big Data by Role of Organisation (n=11)

<table>
<thead>
<tr>
<th>Risk</th>
<th>Operational (6)</th>
<th>Policy (5)</th>
<th>TOTAL (11)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Privacy</td>
<td>3</td>
<td>3</td>
<td>6</td>
</tr>
<tr>
<td>Danger of confusing correlation with causation / Insufficient training</td>
<td>3</td>
<td></td>
<td>3</td>
</tr>
<tr>
<td>Discrimination</td>
<td>2</td>
<td>1</td>
<td>3</td>
</tr>
<tr>
<td>Public perceptions</td>
<td>2</td>
<td>1</td>
<td>3</td>
</tr>
<tr>
<td>Data security / honeypot risk</td>
<td>1</td>
<td>2</td>
<td>3</td>
</tr>
<tr>
<td>Risk of not using Big Data leading to security issues or loss of cost savings</td>
<td>1</td>
<td>0</td>
<td>1</td>
</tr>
<tr>
<td>Accuracy of Data</td>
<td>1</td>
<td>0</td>
<td>1</td>
</tr>
<tr>
<td>Misplaced trust in technology/assumptions behind analytics</td>
<td>1</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Litigation</td>
<td>0</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>Scope creep</td>
<td>0</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>Misuse of data</td>
<td></td>
<td>1</td>
<td>1</td>
</tr>
</tbody>
</table>

*Note: Multiple responses can be coded for each research participant. Not all research participants responded to this question.

**Privacy risks**

Privacy issues were identified as a risk. Curiously, none of the research participants took the view that privacy by design inclusive of de-identification and anonymisation technologies were sufficient to protect privacy in the Big Data era. They thought that privacy enhancing practices and technologies could assist but no one expressed the view that technical measures were by and of themselves wholly sufficient. It was suggested that most people who could understand the possibility of de-identification techniques would know that ‘surely Humpty Dumpty could get put back together again, if necessary.’ (P/P P) This implies that de-identification is only as good as the re-identification restrictions that the law sets.

As one policy research participant put it:

I’m not a huge fan of ... privacy by design or surveillance by design as being the solution to address [privacy] issues. I think that the complexity and the challenges are bigger than that. But at the same time, I mean I do think that it’s clear there are real opportunities.... When we are talking about data usages, for example, that are clearly second generation or third generation off the initial use, how do you obtain appropriate consent for that? ... The answer that, ‘well, don’t worry it’s all de-identified anyway so it’s not personal information’ doesn’t strike me as a fulsome answer. (P/P AA)

When queried as to how privacy issues may be resolved the research participants provided a range of suggestions. There was some consensus that you couldn’t do proper risk analysis because there was insufficient oversight and public awareness to identify the issues. There is little Parliament oversight of intelligence gathering operations where it was stated that ‘Our Parliamentarians are by and large kept in the dark on these issues and the CSE Commissioner and various Privacy Commissioners have attempted many times over the years to get amendments made to the Privacy Act to no avail.’ (O-P/P BB)
Misplaced trust

There was a concern that those people procuring Big Data systems were buying them under ‘the WOW factor like a fast car but no airbags.’ (P-O/P CC). There was a concern about the lack of understanding of Big Data systems, which would either lead to being overly cautious and a risk averse approach where benefits would be limited, or Big Data systems would be used without full appreciation of the types of harm they might deliver.

Discrimination and other harms

Two research participants identified two types of risks that were in their eyes more grave than privacy; these were discriminatory effects, and the general harm that may ensue from the output of data analysis (inclusive of Big Data analysis).

There was one notable comment from someone with decades of data analytics experience where the research participant discussed the risk of working with a wildly inaccurate model:

... [there were] four events that were more than 25 standard deviations from the expected. That’s like – that can’t happen in 10,000 years and they had four of them in a week. That’s a problem. The modelling is ... just assumes that everything is much, much safer than it really is. They’re just not facing up to the downside risk of lots of things. (T/O DD)

Risk of not using big data

One noteworthy risk was the risk of not using Big Data. One research participant commented on the terrible job that law enforcement agencies do at counting crime. Because crime statistics are done so poorly ‘the public now thinks that crime isn’t happening so now we have less money to count crime.’ (O/O EE) The same research participant thought that investment in Big Data systems could improve accuracy of crime statistics and help to deliver better results in resource management. On the latter point, employee efficiency was currently measured in one significant organisation as being categorised as ‘productive’ if you worked the fewest amount of hours with a paucity of additional factors taken into consideration.

Political risks

While some research participants referred to political considerations, none referred to political risks per se. Though one could infer a few points from the research participants and the interviews. When we approached some of the individuals to do interviews, they had originally declined (under a Harper Conservative government). As the interviews took place in Canada during the Federal election it was interesting to see that two of the individuals who had declined wrote back after the election results with a change in governments to say that they now felt that they could do the interviews (post-election with new Trudeau Liberal government). Big Data didn’t present a political risk, consenting to do an interview about Big Data appeared to be a political risk.

Public perceptions

There was a very telling real situation to which some research participants referred regarding the Toronto Metropolitan police collecting and using wifi data at Toronto Pearson International Airport. It was reported in the media that the Toronto police were collecting and using metadata generated through wifi at the airport with speculation that more than metadata being collected such as the content of text messaging and so forth. Those research participants referring to this incident fell into two groups: those with inside information about the event, and those whose information came from the media. One research
participant in the policy group (with former background in operational organisations) describes the Toronto airport incident as:

A good example in Canada where a power-point presentation was leaked and there was an outcry that law enforcement and intelligence were sitting in the airport and login into free wifi. The agency was seeing if they could have the capability, if it worked, and not identifying anyone but that’s not the perception by the media or public. The public doesn’t know that you can’t glean much information from wifi even if it’s open and free. This was a test to see if they could obtain intelligence. The agency never reported why they were doing this even once they were exposed in the media. The public didn’t get the true reason why they were collecting data... This is important part of reassurance to the public. (O-P/P FF)

The above research participant perceived poor communication with the public as a risk, and better communication with the public as a way to manage the risk.

Another research participant stated that you had to ‘be careful because the public’s expectation of our ability to understand and access data significantly differs from capabilities’.

The research participants with internal experience in using capabilities to glean intelligence understood well the difference between testing capability and using capability in an investigation for a purpose. The other research participants saw the airport wifi situation as the agency already having the capability, and that they were using it to extract much personal information about people.

Additional concerns were raised around misuse, more data without better intelligence, and the risk of alienating the public where confidence in policing would be undermined.

Summary and Implications

Invasion of privacy was a risk most frequently nominated by the participants in Canada, and Australia. There were two new risks identified by Canadians: danger of confusing correlation with causation, and litigation. Three out of eleven participants believed that insufficient training / danger of confusing correlation with causation was a risk that could result in harms including privacy, economic and discrimination. One Canadian and one Australian participant also thought that not using Big Data could be a risk.

Overall, the main identified risks related to privacy, data integrity, and general technical issues. Both operational and policy groups expressed the view that there were risks to privacy. A participant who both worked with Big Data on a daily basis and who developed Big Data tools stated that privacy was less of an issue than discrimination. Other participants used the term ‘harm’ to include privacy risks.

2.4.7 Who is exposed to these risks?

Where it was not clear from research participants’ identification of risks, we asked research participants who they felt was exposed to the risks they had identified. The results are shown in Table 2-12.
Table 2-12: Who is exposed to risks of Big Data by Organisation of Participant (n=11)

<table>
<thead>
<tr>
<th>People at risk</th>
<th>Operational (6)</th>
<th>Policy (5)</th>
<th>TOTAL (11)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Everyone/the community/citizens as individuals</td>
<td>3</td>
<td>3</td>
<td>6</td>
</tr>
<tr>
<td>Government decision-making</td>
<td>1</td>
<td>1</td>
<td>2</td>
</tr>
<tr>
<td>Minorities/marginal people/young people/people of certain SES/refugees</td>
<td>1</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>People identified in data/lone citizens</td>
<td>1</td>
<td></td>
<td>1</td>
</tr>
</tbody>
</table>

*Note: Multiple responses can be coded for each research participant. Not everyone responded to this question.

Summary and Implications

‘Everyone’ was the most popular response to who is exposed to risk by research participants in both Canada and Australia. While four participants in the Australian sample identified minorities and marginal people as being exposed to risks, only one participant in Canada mentioned this.

2.4.8 Management of Big Data risks

For the policy group, we also asked ‘How should these risks be managed?’ Some in the operational group gave unprompted suggestions as well, and these have been included. Table 2-13 provides a cross-tabulation of the risks against suggested approaches to the mitigation of these risks. A number of suggested approaches are applicable to several types of risks.

Table 2-13: How Big Data Risks can be Managed (n=5)

<table>
<thead>
<tr>
<th>Risk mitigation via design</th>
<th>Data security</th>
<th>Data integrity</th>
<th>Misuse of data</th>
<th>Privacy</th>
<th>Discrimination</th>
</tr>
</thead>
<tbody>
<tr>
<td>Better public engagement / external transparency</td>
<td>2</td>
<td>1</td>
<td>1</td>
<td>2</td>
<td>1</td>
</tr>
<tr>
<td>Appropriate regulation/ sanctions</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td></td>
<td>1</td>
</tr>
<tr>
<td>Education</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>Law reform</td>
<td></td>
<td></td>
<td></td>
<td>1</td>
<td>1</td>
</tr>
</tbody>
</table>

*Note: Multiple responses can be coded for each research participant. Not everyone responded to this question.

Data security

While most of the research participants mentioned data security as important, few offered specific ways that these risks were managed (e.g. encryption). Although the sample size is small, there seemed to be a perception amongst some of the research participants that there were better risk management practices amongst the private sector than government sectors.

The research participants were consistent in their views that there were many access controls in Canada around data and datasets. A range of types of access controls and risk assessments were stated. One interesting item emerged whereby the types of controls in place for private organisations appeared to be not only more specific but more stringent when compared with government organisations. Here is one response from an individual working in the private sector:
Historically, we have had very strong access controls in place. So it’s very much limited to that need to know premise. We’ve defined it by roles and responsibilities, not necessarily by level in the company. So based on all the data sources that I’ve identified earlier, we’ve been an access control and a sort of tree within each of these Big Data databases and data systems and it’s really released on a need to know basis. What I find, too, with access controls is that they’re not permanent. So it might be — just because somebody is working on a particular project or needs to use data, then they would be able to have access to it.

We also, actually, try not to use live data. That’s one of the protections that we’ve put in place. So rather, that we would take an anonymised data set and do, kind of, the analysis and the building around that data set, rather than using any, kind of, live data.

So we do privacy backed assessments, we do threat risk assessments, we do statements of sensitivity. But I think those are, sort of, some of the outputs. I think, more classically, is that we actually are brought in at the beginning by the project team. To actually sit and have a conversation. We spend time, face to face. (T-O/O GG, emphasis added)

The above quotes are significant in that the participant belongs to an organisation that is both operational and private sector. As will be seen in Chapter 3, private organisations are subject to more regulatory safeguards than government organisations.

Invasion of privacy

While privacy concerns were paramount in research participants’ responses, a few research participants went one step further stating that privacy obligations were generally insufficient and that a more holistic approach to risk assessment is required including privacy, security, compliance and general legal risks.

Other

One research participant thought that one of the greatest risks to the use of Big Data was sale and use of data to third parties. This research participant strongly believed that there should be less third party data sales with tight restrictions around such sale and use. (P-O/P)

Summary and Implications

Research participants discussed a range of potential ways to mitigate against risks. These included access controls more in line with the restraints imposed on the private sector. There was a further suggestion to tighten restrictions on third party data sales. More data security requirements were also suggested as was better education of the public about the actual versus perceived risks of Big Data.

2.5 Regulation

In this section, we analyse the responses of research participants to questions relating to how Big Data as a category, or the access, disclosure, use and destruction of data more specifically, is or ought to be regulated.

2.5.1 Laws, regulation, and internal Guidelines

Research participants with operational, policy or combined roles, and some of those working in technical roles within operational organisations, were asked to identify the legal
framework for the use of data by law enforcement and security agencies. Those whose role was more operational or technical were asked to identify 'laws, regulations or procedures governing the use of data by law enforcement or security agencies' [O20] whereas those whose role related primarily to policy were asked to identify how the use of Big Data was being regulated and ‘the laws, policies, codes of practice, standards etc in place in this jurisdiction’ [P10].

As can be seen in the Table 2-14, the most cited legislation was privacy, C-51/SCISA, and the Canadian Charter of Human Rights and Freedoms. Six participants mentioned agency-specific legislation – mostly from government sector with operational or technical role. Five participants nominated internal documents (such as manuals, guidelines, codes of practice and directives) – all of them were in operational or technical role. A variety of other legislation or instruments were mentioned by one or two participants.

Table 2-14: Legislation and regulatory material identified by research participants according to (1) organisation sector, and (2) type of role (n=11)

<table>
<thead>
<tr>
<th>Category</th>
<th>Private/Research/NGO (n=2)</th>
<th>Independent (n=4)</th>
<th>Government (n=5)</th>
<th>Operational or technical role (n=6)</th>
<th>Policy Role (5)</th>
<th>Total (n=11)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Privacy Act, APPs, provincial privacy laws, Access to Information Act, PIPEDA</td>
<td>2</td>
<td>3</td>
<td>4</td>
<td>4</td>
<td>5</td>
<td>9</td>
</tr>
<tr>
<td>C-51 including SCISA</td>
<td>2</td>
<td>2</td>
<td>4</td>
<td>4</td>
<td>4</td>
<td>8</td>
</tr>
<tr>
<td>Agency-specific legislation</td>
<td>1</td>
<td>2</td>
<td>3</td>
<td>4</td>
<td>2</td>
<td>6</td>
</tr>
<tr>
<td>Canadian Charter of Human Rights and Freedoms</td>
<td>1</td>
<td>2</td>
<td>3</td>
<td>3</td>
<td>3</td>
<td>6</td>
</tr>
<tr>
<td>Internal documents(^1)</td>
<td>1</td>
<td>1</td>
<td>3</td>
<td>5</td>
<td>0</td>
<td>5</td>
</tr>
<tr>
<td>Criminal Code</td>
<td>0</td>
<td>0</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>2</td>
</tr>
<tr>
<td>Security of Information Act</td>
<td>0</td>
<td>0</td>
<td>1</td>
<td>1</td>
<td>0</td>
<td>1</td>
</tr>
<tr>
<td>Dataset-specific legislation</td>
<td>0</td>
<td>0</td>
<td>1</td>
<td>1</td>
<td>0</td>
<td>1</td>
</tr>
<tr>
<td>Competition Act</td>
<td>0</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>Memoranda of understanding</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>International instruments</td>
<td>0</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>Security classification/sensitive information</td>
<td>0</td>
<td>0</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>Archives Act (and retention rules)</td>
<td>0</td>
<td>0</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
</tr>
</tbody>
</table>

\(^*\) Multiple responses can be coded for each research participant, including in the final two rows. Where relevant, categories relate to a former role.

\(^1\) Includes manuals, protocols, guidelines, codes of practice and directives. This specifically includes such documents generated by the Treasury Board.
**Privacy Act**

Research participants consistently referred to how out of date Canada’s privacy laws were for federal agencies noting that the *Privacy Act* was enacted in the 1980s and had not had any significant changes since then in spite of numerous calls for change.

Under the *Privacy Act* non-binding recommendations may be advised in an attempt to improve policies but there is no mechanism to force change. As one research participant described:

... they turn the taps on without ever looking to see if the tap needs to be turned off so there needs to be consequences ... you cannot get a judicial order to cease with a collection practice or to turn the tap off. (P/P FF)

**Bill C-51 / Anti-Terrorism Act**

As previously highlighted, C-51 was an Omnibus Act comprised of a new *Security of Canada Information Sharing Act* (SCISA), and amendments to several other acts. Most of the research participants identified C-51 in the context of SCISA, and not in other contexts. The research participants consistently stated that although Bill C-51 had passed into law, how it would affect their day-to-day sharing of data between agencies remained unknown.

**Treasury Board Policies and Directives**

Federal agencies in Canada receive data governance frameworks from the Treasury Board of Canada. While a few research participants identified the Treasury Board as producing politics and directives around data governance, none of those interviewed went into any detail about the policies and directives.

**Summary and Implications**

| Two regulatory frameworks were identified by the majority of research participants. These were Privacy (*Privacy Act* and privacy frameworks in general) and Sharing (C-51/SCISA). Approximately half of the participants also identified the Charter, and Treasury Board Policies and Directives (these formed the main types of general guidelines for issues) and agency specific legislation. |
| Participants from different roles and sectors equally recognised Privacy legislation, sharing legislation of C-51/SCISA and the Charter. |

2.5.2 **Accountability, transparency and oversight mechanisms**

Accountability issues were mentioned in some of the interviews but transparency and oversight issues were identified in all of the interviews with research participants taking a strong view that more transparency and better oversight was necessary. It is difficult to separate accountability from transparency and oversight given the inter-relationship between these elements.

**Accountability**

Accountability was referred to in three different capacities: data ownership, risk aversion and in an inter-relational manner with transparency and oversight.

Data ownership and accountability was identified as a barrier to Big Data analytics. It was felt by some individuals that government requires that someone ‘own’ the data in order for there to be accountability should things go wrong. Ownership and accountability rest with
an organisation or division. This creates a reluctance to share information across agencies. Sharing bulk data for Big Data would create an even bigger problem with accountability and ownership. The problem of data ownership and accountability was seen to lead to a risk averse culture whereby Big Data and BD analytics would not be taken up quickly or efficiently by governments.

**Transparency**

Some of the research participants saw transparency both as a barrier/risk as well as a potential solution allowing for a better balance between security and civil liberties.

Transparency of algorithms attracted some differing and interesting viewpoints. One research participant went so far as to say that this type of transparency would be valuable, ‘only if you understand what is given to you otherwise there is no utility’ (O-P/P GG).

There was much scepticism as to whether decision makers were capable of making sound decisions based on information gleaned from transparent algorithms. Decision makers have traditionally been trained in social sciences. Decision makers often do not have backgrounds in computer science or information systems. Transparent algorithms require people who have had sufficient training and background to understand what is before them.

**Oversight mechanism**

Only one person in the Canadian interviews thought that there was sufficient oversight of data practices, and law enforcement and intelligence agencies.

There was particular concern over the budget cuts to oversight of intelligence agencies CSE and CSIS. While CSE has a commissioner that oversees its operations, past commissioners have openly expressed their disappointment in that few of their recommendations were taken on board, especially regarding privacy concerns.

Other oversight concerns were perhaps even more alarming. Some research participants highlighted that of the 100 departments and agencies authorised to share information under SCISA only 3 agencies had oversight bodies – CSIS, CSE and the RCMP. There were 17 other agencies with mandates in national security that have no oversight. As one research participant stated:

> There are serious gaps in oversight and operating in silos which is problematic because C-51 is meant to dismantle silos for sharing but there is no dismantling of oversight silos. (O-P/P HH)

Others referred to the lack of an oversight body to oversee the overall data sharing between agencies under C-51. In other words, there needs to be a ‘super oversight body’ to address the totality of information sharing, and not specifically looking from an oversight silo perspective.

Additional concerns were raised about there being a lack of Parliamentary oversight with a culture of secrecy and over-protection lying at the heart of the matter.

**Summary and Implications**

No research participants stated that there was not a need for agencies to share information, especially for national security purposes. All participants save for one believed that there was not sufficient transparency and oversight. Concerns were raised over whether increased transparency would be meaningful absent increased education and training to understand Big Data systems. Algorithmic transparency was regarded as a desirable outcome only if would be sufficiently understood by decision makers.
Information silos were identified at different points in the interviews as concerns. However Canadians also identified the problem of oversight silos and the need for better oversight appropriate for the new form of sharing under SCISA with appropriate resources levels to ensure that oversight is robust.

Curiously, lack of accountability mechanisms were not directly mentioned in the interviews though it is difficult to separate comments about oversight with those of accountability. Accountability issues arose more in the context of culture of data ownership responsibility creating a reluctance to share data. This was discussed as a barrier to governments sharing data, as well as a potential barrier to Big Data uptake.

### 2.5.3 Appropriateness and Effectiveness of Laws and Regulations

In the Canadian study, all research participants were asked ‘In your view, are these laws, regulations, procedures, guidelines (including accountability and oversight mechanisms) appropriate and effective?’ Their responses are captured in Table 2-15.

#### Table 2-15: Evaluation of appropriateness and effectiveness of laws, regulation and oversight by research participants by (1) sector of organisation and (2) type of organisation (n=11)

<table>
<thead>
<tr>
<th>Category</th>
<th>Research/NGO Sector (2)</th>
<th>Independent Sector (4)</th>
<th>Government Sector (5)</th>
<th>Policy Role (5)</th>
<th>Operational and Technical Roles (6)</th>
<th>Total (11)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Negative comments about oversight</td>
<td>1</td>
<td>2</td>
<td>2</td>
<td>4</td>
<td>1</td>
<td>5</td>
</tr>
<tr>
<td>Generally positive with other comment or critique</td>
<td></td>
<td>1</td>
<td>1</td>
<td>2</td>
<td>2</td>
<td></td>
</tr>
<tr>
<td>Positive comments</td>
<td></td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td></td>
</tr>
<tr>
<td>No specific response/unsure</td>
<td></td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td></td>
</tr>
<tr>
<td>Positive or neutral about oversight; negative about restrictiveness, red tape or reduced capacity</td>
<td>1</td>
<td></td>
<td>1</td>
<td></td>
<td>1</td>
<td>1</td>
</tr>
</tbody>
</table>

Note: One research participant did not respond to the question. Two research participants were not asked the question.

#### Summary and Implications

There is no clear division in Canada between sectors. Unlike the case in Australia, there is not a clear division between those in the research/NGO sectors who were sometimes critical (particularly about oversight) and those in the government sector who were generally uncritical, or focussed on restrictiveness. In Australia there were 22 on the positive side with only 3 on the negative side. In Canada this distribution was more equal with 4 positive, and 5 negative. Research participants from all sectors and roles expressed strong concerns with appropriate oversight mechanisms.

### 2.5.4 Perceived Shortcomings in Law, Regulation and Proposals for Reform

Research participants with policy and operational roles were asked to identify shortcomings in the current legal and regulatory regime as well as future strategies for Big Data [P10 d &
Research participants with technical roles were asked what advice they would give policymakers on the use of Big Data or data analytics for law enforcement and national security purposes.

Several participants gave specific comments about gaps in the current legal framework, issues not addressed by current law and how this could be improved. Participants called for amendments to be made to the Privacy Act to be appropriately adapted to both existing and emerging technologies, as well as amendments to SCISA for better oversight. One participant discussing oversight issues suggested that they would:

Address the oversight gaps in some way with expansion of mandates with someone on the group who reviewed (sharing of information) in real time where the oversight bodies always share to get a full picture. Sauce for the goose is sauce for the gander. (O-P/P II)

Others interpreted the question in a different manner calling for more simplified laws and procedures that were more readily understood by both police officers on the street as well as the general public. It followed that more and better education and training was imperative. Another shortcoming was not specifically about a particular law but that the courts were being increasingly called to deal with national security cases and stated that oversight capacity was an emerging issue.

One participant offered:

It’s about integration and being more efficient. The threat environment changes and matters of adjusting rather than is there a huge gap. Each agency has a mandate but how to we operation together, and where is the line between government and national security? (O/O JJ)

Another participant expressed concerns about how metadata is shared with foreign agencies and looking at gaps in the law:

I think we need to put rules around metadata that are not limited to a ministerial authorisation, as we have now, which is very flexible from an operational perspective but doesn’t really provide us with a whole lot of certainly about either what happens or what could or should happen. So there’s an MA (Ministerial Authorisation) around metadata. That’s proven, I think, unsatisfactory, in terms of setting a clearer framework for effective privacy protection and effective oversight. ... I think we need to, on a bilateral basis, or a multilateral basis, spend more time talking about what happens to Canadian data in other jurisdictions. Especially, when you live in Canada, with so much of the data ending up in the United States. [We need] Frameworks from Treasury, next level is Policy, Directives and Standards, Guidelines and Tools. We have a lot of guidelines and rules but how do you harmonise it – trying to reduce the complexity of it. (P/P KK)

It is important to note in that context that research participants’ understandings of the existing legal regime may not be accurate and may not correspond to our, or the governments’ interpretations.
Summary and Implications

Research participants raised general proposals for reform noting that laws around privacy and oversight required updating. There was an additional call for updated Guidelines and Directives for sharing data with foreign agencies in an easier to understand and transparent fashion that could be harmonised across agencies.

Similar to the Australian study, participants called for reduction of the complexity and to enhance harmonisation of practices across agencies. Where research participants from the Australia Study expressed the possibility of reducing ‘red tape’ without reducing oversight, Canadians did not address ‘red tape’ issues. Their concerns were about increasing the oversight framework which is viewed by the majority of participants as inadequate. This may be due to the regulatory framework explored in Chapter 3 where Canada has less restrictions around sharing information when compared to Australia.

2.5.5 Regulation by design

There were three research participants in operational organisations who had a role that enabled them to comment on ‘regulation by design’ within their organisation’s systems. These three participants were asked about the extent to which some of the risks of data analytics could be mitigated through the design of analytical tools as well as the extent to which it was taken into account in their own systems. The three sets of responses are set out in Table 2-16.
Table 2-16: Mitigation of issues/risks associated with data analytics/storage systems through design (n=3)

<table>
<thead>
<tr>
<th>Issue</th>
<th>Participant A</th>
<th>Participant B</th>
<th>Participant C</th>
</tr>
</thead>
<tbody>
<tr>
<td>Privacy and Personal Information Security.</td>
<td>No because it’s taken into account by the person who provides the data. The data is de-identified.</td>
<td>No* Yes. Privacy back assessments, threat risk assessments and statements of sensitivity. Privacy risks analysed from the conceptualisation of the project to the finish.</td>
<td>Yes we use encryption techniques as well as a separate tool to ensure confidentiality</td>
</tr>
<tr>
<td>Communications confidentiality</td>
<td>Physical transfers of data happen when physical reports get handed over.</td>
<td>No Yes. Privacy back assessments, threat risk assessments and statements of sensitivity. Privacy risks analysed from the conceptualisation of the project to the finish.</td>
<td>Yes, designed into the systems.</td>
</tr>
<tr>
<td>Data integrity</td>
<td>Close relationship with data providers. Constant back and forth asking questions. There is a great deal of scrubbing and cleaning to do or “removing the silliness”.</td>
<td>Yes Yes, designed into the systems.</td>
<td>Yes, designed into the systems.</td>
</tr>
<tr>
<td>Regulatory compliance</td>
<td>Yes, Memorandums of Understanding about specific datasets.</td>
<td>Not answered</td>
<td>Not answered.</td>
</tr>
<tr>
<td>Testing and evaluation</td>
<td>No because the produced results don’t represent risk or anybody in particular.</td>
<td>Yes Yes. We do not use live data.</td>
<td>Yes Yes. We do not use live data.</td>
</tr>
<tr>
<td>Unintended consequences</td>
<td>Unintended consequences are key results that shouldn’t be avoided. They produce the added value of Big Data.</td>
<td>Not answered</td>
<td>Not answered.</td>
</tr>
<tr>
<td>Avoiding discrimination</td>
<td>Doesn’t occur in the context of organisation’s work but in the bigger picture is seen to be a significant problem.</td>
<td>No Yes, discussion where individual case may yield an outcomes with discriminatory consequences</td>
<td></td>
</tr>
<tr>
<td>Agency interoperability</td>
<td>Movement towards using data intelligently</td>
<td>Yes No</td>
<td></td>
</tr>
<tr>
<td>Re-identification risk</td>
<td>Impossible to make data unidentifiable; this can always be done.</td>
<td>Yes Possible but I’m uncertain.</td>
<td></td>
</tr>
<tr>
<td>Cost</td>
<td>Yes, when purchase consider value for money and appropriateness of package</td>
<td>Yes Yes</td>
<td></td>
</tr>
</tbody>
</table>

* With some of the interviews there wasn’t time left to answer these questions in greater detail. The questions may have been answered merely ‘yes’ or ‘no’.
Summary and Implications

Data integrity and cost were the only three design features that were taken into account by each of the three research participants, all having worked in operational organisations. This suggests that data practices are not unified across departments. The question about privacy by design yielded an interesting result where one organisation placed this responsibility with the data owner, another said that they didn’t factor in privacy, while the last research participant laid out extensive measures used to assess and minimise privacy concerns.

2.6 Values and Big Data

In Australia, much of the debate about appropriate legal and regulatory regimes lies in different attitudes and values. Different values and different sources of information can yield divisions between those working in government, particularly in operational roles, and those working on policy in the research/NGO sector. In particular, different people can have different views on the role of consent of data subjects, on the importance of privacy and particularly whether it ought to ‘give way’ to security, and on the need for and importance of transparency in operational contexts. We thus asked research participants with policy roles a series of questions seeking to understand their position in these debates, as well as the sources of their views and understandings, the extent to which they perceived their views as in conflict with others and how they would address any such conflict.

In Canada the policy research participants presented a unique situation in that three out of the five people interviewed had previous experience working in intelligence agencies, oversight bodies, and law enforcement. They now, however, had roles in their current positions that were policy-orientated.

2.6.1 Protections where individual consents to use or sharing of their data

The Policy group were asked specifically for their views on an important policy question, namely ‘what protections, if any, should remain in place in circumstances where an individual consents to the use or sharing of their data?’ The different categories of responses among the policy group did not mirror as closely as those in the Australian sample.

Consent is important. All five research participants found consent to be important but none thought that how consent currently works is adequate.

Consent needs to be active, clear and visible, fully informed and unpressured. Three of the research participants emphasised the need for informed/real consent.

Consent needs to be opt-in and not implied. Two research participants identified the need for opt-in consent versus opt-out consent. One research participant elaborated further calling for both opt-in and express consent noting that the trend was one of implied consent and opting out.

Data must be used for a proper purpose. Only one research participant discussed that consent should only be for when data is used for the purpose of collection, access and use and argued that there should be less third party data sales. Another research participant stated that consent does not replace the authority to collect or use information that isn’t directly tied to your organisation’s mandate or authority.
Summary and Implications

As in Australia, research participants mentioned issues around the ‘quality’ of consent, continuing limits on its use (including proper purpose). The issue of expiry or revocation was raised by both Australian and Canadian research participants. Two Canadian research participants expressed concerns over implied and opt-out standards calling for opt-in and express consent.

2.6.2 Attitudes to privacy

Participants were asked to comment on the balance between privacy and threats such as child kidnapping, child sexual abuse or terrorism. Table 2-17 summarises their responses.

Table 2-17: Policy participants’ attitudes to privacy by organisation sector (n=5)

<table>
<thead>
<tr>
<th></th>
<th>Research/NGO/ Private (2)</th>
<th>Independent (2)</th>
<th>Government (1)</th>
<th>Total (5)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Privacy should give way in the face of such threats (if justified)</td>
<td>1</td>
<td>1</td>
<td>2</td>
<td></td>
</tr>
<tr>
<td>Need to find balance in circumstances</td>
<td>1</td>
<td></td>
<td>1</td>
<td></td>
</tr>
<tr>
<td>Need to follow rules (including oversight, necessity and proportionality requirements)</td>
<td>1</td>
<td></td>
<td>1</td>
<td></td>
</tr>
</tbody>
</table>

* Multiple responses can be coded for each research participant. One research participant didn’t answer the question.

Summary and Implications

As in the case of Australia, there are varied views on the importance of privacy, particularly in the context of serious imminent threats. No-one expressed the view that privacy should always be prioritised.

2.6.3 Privacy versus Security: A scenario

In order to gain greater insight into the ways in which research participants with policy or joint operational/policy roles believed that concerns around privacy (including surveillance) do or ought to interact with concerns around security, we presented research participants in that group with a scenario:

Lucy is an 8 year old girl who has been kidnapped from her home in Ottawa. All avenues of traditional physical surveillance and canvassing of the area so far haven’t produced any leads. How do you feel about the immediate and expeditious use of Big Data tools in these circumstances?

This was essentially what this question set out to test. After an initial response to this scenario or where the research participant asked for examples, and in order to further test where research participants would draw lines, research participants were asked a series of more specific questions, in particular their response to:

a) A metadata (secondary data) search of all known kidnappers with previous arrests in the area matched against CCTV footage from public and private sources in Ottawa on the day of the kidnapping.
b) Collection of data and monitoring of all known kidnappers including known addresses, registered telephonic devices, social media accounts and email accounts

c) Facial recognition deployed on CCTV footage across all Sydney and surrounding areas, and multiple social media networks, in an attempt to identify Lucy

d) Metadata from all devices of all family members of Lucy, her neighbours, and people seen visiting the house that day (including a postal worker, package delivery service, water meter inspector).

Table 2-18: Responses to general kidnapping scenario and specific prompts (n=5)

<table>
<thead>
<tr>
<th></th>
<th>Agree to use tool/s</th>
<th>Agree to use tool/s with caveats</th>
<th>Reluctant to use tool/s</th>
</tr>
</thead>
<tbody>
<tr>
<td>Initial response</td>
<td>1</td>
<td>2</td>
<td>0</td>
</tr>
<tr>
<td>Prompt (a)</td>
<td>1</td>
<td>2</td>
<td>0</td>
</tr>
<tr>
<td>Prompt (b)</td>
<td>1</td>
<td>2</td>
<td>0</td>
</tr>
<tr>
<td>Prompt (c)</td>
<td>1</td>
<td>2</td>
<td>1</td>
</tr>
<tr>
<td>Prompt (d)</td>
<td>1</td>
<td>2</td>
<td>1</td>
</tr>
</tbody>
</table>

* One research participant in the policy group was not asked this question due to time constraints.

** Some respondents mentioned general caveats in giving a positive response initially. Where these were repeated in relation to specific prompts (including by reference), the research participant was placed in the ‘agree to use tool with caveat’ column. However, where the research participant did not mention the earlier general caveat but gave an unconditional positive response to the prompt, they were put into the ‘agree to use tool’ column.

The answers to the scenario were significantly briefer than those interviewed in Australia.

Three research participants identified that under Canadian law all of these scenarios including the prompts would not present an obstacle to using Big Data tools to help find Lucy. However, two of the research participants were uncomfortable with the use of Big Data tools due to potential for scope creep and abuse, and that the initial collection of data was done within a legal framework where privacy considerations are inadequate.

Summary and Implications

Three of the Canadian research participants gave the same answers to the scenario whether the context was kidnapping, child sexual assault or terrorism. They indicated that there are sufficient legal provisions and flexibility to allow law enforcement to move to more intrusive measures in order to curtail the threat. Only two participants indicated potential problems such as abuse or scope creep, and only one participant was uncomfortable with the use of Big Data techniques including the escalation of context but these were recorded as using tools with caveats.

2.6.4 What transparency is required?

We asked research participants with policy roles and joint operational/policy roles to comment on the extent to which there should be transparency about the nature of data collected or the algorithms employed in analysis, both within an agency and more broadly.

We asked three questions around transparency to policy organisations: ‘To what extent should there be public transparency about: a) the nature of data, b) the algorithms, and c) intra-agency transparency of data and algorithms? Table 2-19 highlights the responses for the four research participants.
Table 2-19: Transparency

<table>
<thead>
<tr>
<th></th>
<th>Participant A</th>
<th>Participant B</th>
<th>Participant C</th>
<th>Participant D</th>
</tr>
</thead>
<tbody>
<tr>
<td>Nature of Data</td>
<td>Yes</td>
<td>Yes and this is a legal obligation.</td>
<td>Yes</td>
<td>Yes, very transparent</td>
</tr>
<tr>
<td>Algorithm</td>
<td>We need more algorithmic transparency for sure. The challenge is how do we get to that point.</td>
<td>Only if you understand what is given to you otherwise there is no utility.</td>
<td>Yes but only to the extent that it’s useful so it needs to fall before educated eyes. Helpful would be explaining to the public how we collect and use data. Unhelpful would be at the level of algorithmic warrants.</td>
<td>Yes. Open about the what but not the how as you don’t give away your tools.</td>
</tr>
<tr>
<td>Intra-Agency</td>
<td>Yes of course</td>
<td>Hugely important and in fact there needs to be clear information sharing criteria agreements.</td>
<td>Yes but there are limits.</td>
<td>Without data transparency you won’t get the sharing that you need (between agencies).</td>
</tr>
</tbody>
</table>

Responses between the four research participants yielded a consistent “yes” to all three transparency questions: data, algorithm and intra-agency. Three research participants highlighted the need to limit transparency about algorithms to situations where it would be useful and where it would be understood.

**Summary and Implications**

Transparency is a challenge for national security and law enforcement agencies. Transparency can ensure that errors and biases are addressed, is a deterrent to misuse of data, is an important public value, and is an important element of democratic accountability. However, operational secrecy is also crucial for effectiveness in many situations.

Unlike in Australia, the four research participants who responded were not concerned about competing priorities in increasing transparency. In the Australian study there were differences in attitudes between transparency of the data and transparency of the analysis itself. In Canada there was no differentiation. The Canadian responses instead focussed more on utility, education, limits and the importance of trust and rules when sharing information between agencies.

2.6.5 How views align with others

Research participants with policy and joint operational/policy roles were asked to comment on how their views about the design and regulation of Big Data aligned with the views of other stakeholders. This question produced some answers previously unseen in the Australian study.

One research participant commented that
I think that our organisation is clueless so it’s moot. Individual analysts may have some commonality but at the organisational level, this doesn’t even cross their threshold. (P/P LL)

Another jokingly commented that, ‘Nobody agrees with anything that I say.’ He then further added that a qualification:

When you talk with law enforcement or security officials, they come at it from a perspective and experience of seeing things that I haven’t seen, so often have deeply held convictions that create barriers or by and large are a significant problem and you’ve got to understand the harm that’s taking place. You should be able to do what’s needed to be done. We’re the good guys, kind of thing, so to speak. Equally, there are people on the privacy side who I deal with from time to time who see the cops as the bad guys, at the end of the day, quite frankly, and are deeply sceptical about almost all of this stuff... I’m not in either of these camps. (P/P MM)

Other interviewees characterised their alignment with stakeholders as taking a broad approach to the issues as well as a cautious approach.

Summary and Implications

The views reflected in the Canadian sample were different from those in the Australian sample. In Australia, research participants formed four clusters (rights-based NGOs and community groups, victim-aligned NGOs, industry groups, and government agencies) whereas in Canada rights-based NGOs and community groups, or victim-aligned NGOs were not interviewed. In Australia, differences could be explained in part by the fact that different sectors have different levels of knowledge about how data is actually used and how this use is regulated. In Canada, however, this distinction was not as apparent. This could be due to the fact that three out of the five policy research participants had previous roles in intelligence and law enforcement such that their views would have been formed from having seen the issues develop from different perspectives.

2.6.6 Conflict of Values

Canadian research participants did not provide responses to this line of inquiry.

2.6.7 Source of views

Having asked research participants with policy roles about their views on various issues, we asked them to identify the sources of the views, in particular the extent to which they were shaped by internal or personal experience as opposed to external sources (such as blogs, watch groups and media) [P20]. Table 2-20 provides a breakdown of the sources by sector.
### Table 2-20: Sources of views of Policy group by organisation sector (n=5)

<table>
<thead>
<tr>
<th>Source of View</th>
<th>Private/ Research/ NGO (2)</th>
<th>Independent (2)</th>
<th>Government (1)</th>
<th>Total (5)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Professional/personal experience, knowledge</td>
<td>2</td>
<td>1</td>
<td>1</td>
<td>4</td>
</tr>
<tr>
<td>Evidence / Academic papers / Reports</td>
<td>2</td>
<td>1</td>
<td>1</td>
<td>4</td>
</tr>
<tr>
<td>Media/blogs</td>
<td>2</td>
<td>1</td>
<td>1</td>
<td>4</td>
</tr>
<tr>
<td>Broad consultation</td>
<td>1</td>
<td>1</td>
<td></td>
<td>2</td>
</tr>
<tr>
<td>Contact with experts</td>
<td>1</td>
<td>1</td>
<td></td>
<td>2</td>
</tr>
</tbody>
</table>

* Multiple responses can be coded for each research participant.

**Summary and Implications**

Four out of five research participants reported three main sources of their views: professional or personal knowledge, evidence or academic papers/reports, and media/blogs, two nominated ‘broad consultation’, and two ‘contact with experts’. Compared with the Australian sample, the Canadian research participants appeared to rely more on sources of information external to their professional or personal experience.
3. BIG DATA, LAW ENFORCEMENT AND NATIONAL SECURITY: THE LEGAL ENVIRONMENT IN CANADA

This chapter discusses features of the Canadian legal framework relevant to Big Data, law enforcement and national security.

The chapter is divided into eight sections that reflect the lines of inquiry introduced in Chapter 5 of the Methodology Report, generally referred to as the 'lens' in this discussion. The sections therefore address aspects of the regulatory framework on the following questions:

1. Is access for data mining enabled?
2. Are legal controls comprehensive and proportionate?
3. Are legal rules clear, principle-based, consistent and instructive?
4. Is integrity of data and systems supported?
5. Are data and systems protected?
6. Is accountability maintained?
7. Are principles and rules regularly reviewed?
8. Is there a sufficient measure of transparency?

While the ‘lens’ is used to structure this discussion, it is important to emphasise that it is only used to inform the lines of inquiry, and not as a tool to assess the current framework. It is used to focus the inquiry on key elements which, if collectively present, would be indicative of a framework that:

- supports the effective use of advanced analytics and large data sets for law enforcement and national security purposes,
- while respecting the rights and interests of all stakeholders (including data subjects and the broader community and economy);
- reflects proportionality and evidence-based justification and decision-taking; and
- ensures comprehensive identification and management of risk and opportunities.

The indicators are not presented as a comprehensive or final list. While they provide structure to the analysis, it is not meant to restrict the broader enquiry or the ongoing debate about an appropriate framework.

3.1 Is access for data mining enabled and are legal controls comprehensive and proportionate?

The first and second lens principles were combined because differentiation in the legislation is made between the types of organisation that wishes to collect, use, and disclose data. These organisation types are: government agencies (inclusive of law enforcement), private organisations, intelligences agencies, and foreign agencies. It is difficult to analyse access to data and data-mining separately from controls around data use, access and controls are therefore considered together.

The first line of inquiry addresses access to data, subject to the governance and control mechanisms set out in 3.3–3.8 below, for purposes of analysis using Big Data techniques. It considers whether the framework enables access, subject to those mechanisms, to relevant datasets held by government agencies (domestically and internationally), to open source data and to relevant privately-held data in a manner that allows data mining.

The legal framework would enable access to relevant datasets held by government agencies (domestically and internationally), to open source data and to relevant privately-held data in a manner that allows data mining, subject to the governance and control mechanisms.
The inquiry into access to data also extends to the use and abuse of mechanisms such as encryption, for instance key escrow and end-to-end encryption.

In Canada, access to government datasets, open datasets and privately-held data is allowed provided that a specific instance is not prohibited under a legislative provision. As will be seen in the legislation and Treasury Board Policies and Directives, there are no binding instruments that directly prohibit access for data mining or similar uses provided that the data-mining is not done as part of an investigation. There is no mention of bulk datasets. The requirements around data-mining can be seen as soft control.

There is no publicly available binding framework around encryption or key escrow (though one may apply to a court to obtain a public key to a technology such as a type of mobile phone, or to a specific device), but controls such as de-identification of data are present. Intelligence agencies would have protocols around encrypting sensitive information, but these are not made available to the public. There are, however, Treasury Board issued security standards of which encryption is an option for agencies to implement depending on their risk assessments.23 There are many controls around data as will be seen in the next Lens principle below.

Much of the Canadian law around data access, mining and controls for government agencies was written in between 1983 and 1985 with no amendments since then, making it difficult to relate issues such as privacy protection to aspects of advanced technologies and forms of data collection. As we have already seen in the interviews there is a uniform concern around privacy and oversight with call for urgent amendments to the Privacy Act. The Treasury Board Policies and Directives, however, do provide some useful guidance around data governance and privacy which will be examined in this and subsequent sections.

As will be demonstrated below, the controls around data mining and analysis are piecemeal and at times confusing and inconsistent. This is largely because the Privacy Act and many of its related policies and directives are out of date.24 Data analytics is not the subject of any one policy, directive or legislation.

There are no references to Big Data in Canadian legislation and policy (no surprise as there aren’t in Australia either), or the use of bulk data sets. There are also a few government institutions that publicly recognise that they are using Big Data analytics (although no publicly available references to the use of Big Data in the national security space).

The discussion in this section looks at different parameters for access to data mining or its equivalent along with the controls in place around data governance. Canadian legislation differentiates between the classification of an organisation, and not between different types of data with the exception of health data. For instance, the regulations do not refer to government-held data, privately-held data, open data and foreign-held data.

The general rule in Canada is that if data collection, use, and sharing are not prohibited by law, then there is great legal latitude for data access, collection, use and sharing. As will later be explored, intelligence agencies have less controls imposed than law enforcement agencies. There are few legal restrictions around the use of open data for law enforcement and intelligence data practices within Canada. Data practices between foreign entities have some restricting principles, but most of what goes on in the intelligence space is neither

---

publicly available nor fully available to oversight bodies, including the Federal Court. This is analysed in greater detail below.

### 3.1.1 Federal government agencies

**Privacy**

Data practice for all Federal government agencies is regulated externally under the *Privacy Act*. The Privacy Act addresses ‘an individual’s right to access and correct personal information the Government of Canada holds about them or the Government’s collection, use and disclosure of their personal information in the course of providing services (e.g., old age pensions or employment insurance).’ Federal agencies are able to collect, use, share, retain and dispose of information subject to several general principles. Where information is ‘personal information’ a number of principles are required around the use of the information. These principles are similar to Australia but are not as comprehensive as either the Australian Privacy Principles or the privacy principles that are binding on federal private sector under PIPEDA. Only collection and use, as well as disclosure are examined below.

**Collection and Use**

Personal information may only be collected if that information relates to the agency/organisation’s operating program or institutional activity. It reasonably follows that data mining involving personal information can be done only if it is related to that agency’s mandate. This does not mean, however, that an agency is restricted from data mining third party data such as open data; it merely means that when an agency itself collects data it must be in relation to its institutional activity.

**Disclosure**

Disclosure of personal information to a third party is generally prohibited absent consent from the individual. There are, however, a number of specific exemptions including information disclosure for:

- Audit purposes,
- Any Aboriginal government for research or to validate a claim,
- Archival purposes,
- Subpoena or warrant,
- Investigations (curiously this isn’t defined in the act in any way to delineate between different types of investigations or those by law enforcement, intelligence or other).
- Prosecution (public and criminal though no differentiation is made in the act itself),
- Civil proceedings against the Crown or the Government of Canada,
- Identifying an individual who owes debt to the government, and
- Where it is in the public interest to disclose.

27 The Australian Privacy Principles (APPs) are contained in schedule 1 of the *Privacy Act 1988* (Cth).
29 *Privacy Act*, R.S.C., 1985, c. P-21, s 8(1).

(cont.)
The *Privacy Act* makes it clear that disclosure is allowed if there is a warrant or subpoena. Disclosure is also permitted in the course of an investigation, prosecution or in civil proceedings. As we’ve previously seen in the decisions of *Jarvis, Spencer and Wakeling* in Chapter 1, the courts have specified that information access, use and disclosure leading to investigation and prosecution require a warrant or equivalent judicial authority.

Collection of personal information does not require an individual’s consent where the information is used for the purpose of which the information was obtained. Consent for another use requires consent or must meet the requirements in subsection 8(2). The Act does not contemplate if an agency may use personal information collected for a different use for which it was collected (or outside of its mandate) if the information is de-identified.

One section of the *Privacy Act* in particular is potentially problematic when put in the context of Big Data. Section 8(2)(j) states that information may be disclosed:

(j) to any person or body for research or statistical purposes if the head of the government institution

(i) is satisfied that the purpose for which the information is disclosed cannot reasonably be accomplished unless the information is provided in a form that would identify the individual to whom it relates, and

(ii) obtains from the person or body a written undertaking that no subsequent disclosure of the information will be made in a form that could reasonably be expected to identify the individual to whom it relates.

This section does not prohibit disclosure of ‘personal information’ under two conditions: purpose of disclosure requires identified information and where there is an undertaking for no further disclosure. There is nothing in the *Privacy Act* that addresses when de-identification of data is required in data-mining or for disclosure to another agency. One assumes that agencies may share de-identification information as there is nothing that prohibits this directly in the statute. The decision in *Jarvis*, however, tells us that sharing identified information between government agencies for the purpose of an investigation requires a warrant.

On the one hand, if personal information is de-identified, other organisations may use the data. On the other hand, if the de-identified data is later used to identify an individual in the course of an investigation leading to criminal charges, a disclosure problem arises if a warrant has not been obtained. This potentially creates a dilemma for Big Data where de-identified data is used. The difficulty is that the section identifies a potential problem with the use of de-identified data, or data not initially associated with an identifiable individual. While de-identification of data relating to individuals is possible (identifying elements can be stripped out or otherwise rendered less useful for identification at the point of collection, before uptake), and some data records are not easily identified with an individual in the first place, the more data is collected and the more analytical tools come into play, the more likely re-identification becomes.

The possibility that de-identified data may be re-identified poses a challenge for the structure of privacy legislation, in Canada as elsewhere. In the Canadian *Privacy Act*, section

31 *Privacy Act*, R.S.C., 1985, c. P-21, ss 8(2)(c) and 64(1)(a)(i).
33 *Privacy Act*, R.S.C., 1985, c. P-21, s 64(1)(b).
8(2)(jj)(ii) implies that information is personal information if it ‘could reasonably be expected to identify the individual to whom it relates.’ Given ongoing developments in re-identification tools, this may mean that data will rarely be sufficiently de-identified to fall outside privacy protections.

There are no legal requirements in the Privacy Act around appropriate consent, and it is silent on data mining.

Sharing

There are two main sharing resources in Canada both operated by the RCMP. These are and the Police Reporting and Occurrence System (PROS) and the Canadian Police Information Centre (CPIC). The RCMP is responsible for the databases which means that they are the facilitators of data exchange between different agencies, and within different departments of their own agency. They also have developed the data polices (not public information) related to the storage, retrieval and communication of data. Agencies share information based on individually negotiated Memoranda of Understanding (not publically available). The RCMP has the primary obligation to protect the privacy of individuals and guidelines and MoUs exchanged between agencies must include parameters around data exchange.

PROS is a police records management database operated by the RCMP that is used both by the RCMP and other partner agencies (23 agencies in 2011). This records management system contains information about suspects, victims, witnesses and offenders who have come into contact with police. The database records the chain of contact from the first moment an event happens (contact with police) along the investigation up to the final result such as if an incident goes to court.

CPIC has many databases such as “drivers’ licences and vehicle plates, stolen vehicles and boats, warrants for arrest, missing persons and property, criminal history records, fingerprints, firearms registration and missing children”. While these databases mostly contain personal information and data on individuals in Canada, some databases include information from the United States and Mexico (Eg. Such as the driver’s licence and vehicle plates database. CPIC holds millions of records.

PROS and CPIC data bases are not the only databases used by various government agencies. Agencies may negotiate use of other agencies databases through Memoranda of Understanding. For example, the RCMP in British Columbia has access to British Columbia Correction Services databases. Some researchers at Simon Fraser University and the Royal Military College (there may be others) also have access to such databases. Some SFU researchers have access to RCMP databases while some researchers at the Royal Military College have access to Correction Services databases. All agencies may acquire and use data (where de-identified or where there are Memoranda of Understandings) from Statistics Canada.

Authorised individuals may perform queries across multiple data sets through the 2012 implemented Integrated Information System (IIS). IIS provides improved access measures and multiple query searches across various databases including PROS, Police Reports Information Management Environment for the province of British Columbia, Major Case

Management, National Criminal Databank, and Automated Criminal Intelligence Information System. IIS is said to compile both structured and unstructured data from the above databases. IIS is accessed by intelligence agencies in Canada and RCMP Operations as well as external law enforcement partners for ACISS (partners are not specified).

The Security of Canada Information Sharing Act 2015 (SCISA) shields participating government agencies from civil liability arising from information sharing and creates a framework to encourage information sharing. SCISA does not mandate information sharing, not even between CSIS, CSE and the RCMP. It merely allows and encourages information sharing between agencies. Section 3 of the Act states that ‘the purpose of this Act is to encourage and facilitate the sharing of information...’. Information disclosure as such is allowed ‘in respect of activities that undermine the security of Canada, including in respect of their detection, identification, analysis, prevention, investigation or disruption.’

Ironically, information sharing between the agencies identified in SCISA was not prohibited prior to this Act. The Act provides legal clarity designed to break down silos, foster information sharing and facilitate more effective operations in the national security space.

Section 4 of SCISA creates broad control measures. The two most relevant to Big Data are:

- respect for caveats on and originator control over shared information is consistent with effective and responsible information sharing; 39
- the provision of feedback as to how shared information is used and as to whether it is useful in protecting against activities that undermine the security of Canada facilitates effective and responsible information sharing 40

If information is shared with another institution the information owner is allowed to place caveats on how that information may be subsequently used. It remains to be seen what caveats might be appropriate for exchange of bulk data sets or requiring that data analytics be performed for a particular purpose. SCISA does not openly contemplate bulk data sets. There is nothing in the legislation to suggest that bulk datasets are included or excluded. Feedback also provides another control mechanism but the Act is silent as to who performs and receives feedback. Further, as there is no oversight body to oversee information sharing amongst SCISA organisations, it remains to be seen whether the feedback loop will be effective.

Absence of access and privacy controls

The Canadian framework on access control may be readily contrasted with both the Australian and United Kingdom’s frameworks where governments are bound to respect various data protection principles. There is a lack of articulated legislative control measures in Canada for Federal agencies’ use of data with the exception of information sharing between agencies involved with security threats. The controls for law enforcement (but not intelligence agencies) are found in the case law of Wakeling, Jarvis and Spencer. The only control specified in these decisions is, however, that a warrant is required to access, use and disclose information if done in the course of an investigation leading to charges. This does

39 Ibid, s 4(b).
40 Ibid, s 4(d).
41 Ibid, s 4(b).
not mean, however, that agencies are over-sharing data or abusing privileges; it simply means that legislative controls are minimal.

That said, the courts have intervened to deliver a clear and consistent message that controls are necessary to safeguard against privacy invasion and human rights violations. As was seen in the cases of *Spencer, Jarvis,* and *Wakeling,* law enforcement will be required to obtain a judicial warrant or court order to access and use many forms of data including telecommunications metadata for the purposes of criminal investigation.

Law enforcement agencies also require a warrant to access or intercept the content of private communications such as emails and texts as explored below. A warrant is also required to access communications that are stored such as those found in the cloud or on a device. Here an interception warrant is required to view the content of a private communication. The definition of ‘private communication’ is of interest. A private communication, as defined in Part VI, s 183 of the *Criminal Code,* states:

\[
\text{private communication means any oral communication, or any telecommunication, that is made by an originator who is in Canada or is intended by the originator to be received by a person who is in Canada and that is made under circumstances in which it is reasonable for the originator to expect that it will not be intercepted by any person other than the person intended by the originator to receive it, and includes any radio-based telephone communication that is treated electronically or otherwise for the purpose of preventing intelligible reception by any person other than the person intended by the originator to receive it} \ldots
\]

In Canada, the location of the intended recipient plays a role, as opposed to a strict definition of someone or a device being physically located in Canada. ‘Stored communications’ is not a term that is used in the Canadian framework, and is not defined in the *Criminal Code.*

Interception warrants are granted by judges of a superior court (called a s 96 court in Canada as they refer to s 96 of the Canadian Constitution allowing judges to be appointed to the provinces and federal courts) in confidential hearings. Similar to Australia, interception warrants require the applicant to outline a number of items including the facts given rise to suspicion, type of communication to be intercepted, names, number of instances, and so forth.\(^{42}\) One item of difference involves notification that a suspect has been made the target of an interception. Section 196(1) of the *Criminal Code* requires that the target(s) of surveillance must be notified within 90 days once the warrant or authorisation has expired unless it is in the ‘interests of justice’ not to disclose the surveillance. In the latter circumstance (notably in cases of terrorism) the confidentiality element may be extended for up to three years under s 196(2).

The Canadian system differentiates between accessing communications stored on a device and accessing communications stored on a third party server such as an Internet Service Provider or cloud space. An interception warrant is required to access communications stored on a third party server, while an information search warrant is required pursuant s 487 of the *Criminal Code* to access communications stored on a device.\(^{43}\) This distinction, of course, makes little sense when communications are stored on a device and on a server but is, nonetheless, Canadian law at present. Search warrants and production orders (to

\(^{42}\) *Criminal Code,* R.S.C. 1985, c. C-46, s 184(3).

\(^{43}\) The type of required warrant for the RCMP to use was contested in the Supreme Court in *R v Telus* (2013) SCC 16.
preserve data) pursuant to s 487.02 do not refer to communications but to data. This differentiation is confusing in that it does not distinguish between mere data (computer data, transmission data, tracking data) and the content of private communications.

Intelligence agencies are not bound by the same controls for data collection, use and interception.

**Controls set out in Treasury Board policies and directives**

Federal Government agencies data practices (Information Management) are largely derived from policies set and made by the Treasury Board of Canada. As stated on the Treasury Board website: ‘Information management is a discipline that directs and supports effective and efficient management of information in an organization, from planning and systems development to disposal and/or long-term preservation.’

The binding nature of Treasury Board policies and directives is complex and largely ambiguous. The courts have on numerous occasions unequivocally stated that such policies and directives are binding with regards to employment laws, pensions and contractual agreements and the like. Other areas such as privacy related guidelines can be seen as soft law, or as providing guidance in interpreting legislation, but the policies themselves are not binding. Additionally the organisation itself (such as the Canadian Radio-Television and Telecommunications Commission, CRTC) may decide to bind itself to such policies in a more substantial manner. As will be seen below, the policies themselves are largely general principles so there is great leeway in how an organisation implements such policies.

The decision *Canada (Information Commissioner) v. Canada (Commissioner of The Royal Canadian Mounted Police)* addressed the issue as to whether the Court should turn to the Treasury Board for guidance in interpreting s 3 of the Privacy Act and s 19 of the Information Act and, in particular, look to the Treasury Board Manual on Access to Information. It was held that the Manual is to be given less weight in evaluating legislative instruments. The Court further noted that Guidelines and Directives, however, would be given more weight than mere manuals for interpreting privacy principles, but the court does not go into detail in terms of how binding or how influential Treasury board Guidelines and Directives may be in this sphere.

The Treasury Board’s website provides a comprehensive list of Directives and Standards to be applied to information management. There is a hierarchy commencing with a Canada wide strategy called the Policy on Information Management. One of the key goals in the strategy is to harmonise information management practices across government departments. The Treasury Board has published hundreds of policies and directives.

---


45 There are over 5000 cases concerning Treasury Board policies and disputes over employment law. For two recent examples see *Meredith v. Canada (Attorney General)* [2015] 1 SCR 125; and *Professional Institute of the Public Service of Canada v. Canada (Attorney General)* [2012] 3 SCR 660.

46 Canada (Information Commissioner) v. Canada (Commissioner of the Royal Canadian Mounted Police) [2003] 1 SCR 66.


48 Treasury Board of Canada, *Policy on Information Management* (1 April 2014), s 5.1.

(cont.)
The most relevant of the above policies for data-mining are Standard on Privacy and Web Analytics, and Standard on Metadata.49

**Privacy and Web Analytics Standard**

This standard discusses requirements, roles, responsibilities and consequences for Web analytics.50 There are three main areas:

1. Collection, use and retention of personal information by government institutions for Web analytics.
2. De-identification of information prior to storage.
3. Disclosure of transmittal of personal information for purposes of Web analytics to a third-party service provider.

Use of personal information for profiling of individuals is prohibited. There are no specific policies or directives for data analytics or Big Data analytics, only Web analytics. Here the various requirements refer to Web analytics (one assumes this means the Internet and is not limited to the technical protocol World Wide Web). Many of the controls are around notification of cookies and similar website trafficking tools, privacy policies, and refers to personal information mainly in the context of Internet Protocol addresses. ‘Web Analytics’ are defined as ‘the collection, analysis, measurement and reporting of data about Web traffic and user visits for purposes of understanding and optimizing Web usage.’51

In as much as Big Data may be concerned with data around Web traffic, the controls that are in place require de-identification of data prior to storage, data retention for a maximum of 18 months, data destruction once 18 months has lapsed, and privacy notices of information practice. Where Web analytics are done externally by a third party, notification to the data subject is required, data may only be retained for six months, after this period has lapsed the data must be destroyed, and there must by a contract in place whereby the third party understands the appropriate privacy protections pursuant to Treasury Board directives and policies, specifically The Directive on Privacy Practices and the Policy on Privacy Protection. The contract must contain:

A requirement that the third party be prohibited from using techniques such as, but not limited to, interlinking, cross-referencing, data mining or data matching from multiple sources on the personal information collected in relation to the work, unless expressly pre-authorized to do so, in writing, by the government institution.52

Data mining is expressly prohibited by third parties performing web analytics for government institutions unless there is express pre-authorisation. By default, data mining, matching and other analytics done internally are not prohibited, and therefore authorised. This particular policy on Web analytics controls apply to those entities in section 3 of the Privacy Act which sets out an exhaustive list of government institutions in Schedule 3. CSIS, CSE, the RCMP and virtually all institutions involved with national security are listed. Crown Corporations such as Canada Post must also comply with the Web Analytics Standards53.

---

50 Treasury Board of Canada, *Standard on Privacy and Web Analytics* (31 January 2013)
51 Treasury Board of Canada, *Standard on Privacy and Web Analytics* (31 January 2013), Appendix C.

(cont.)
There is no Treasury Board Directive or Policy on Data Analytics, Big Data or use of bulk datasets. The metadata standard, as seen below, is concerned with uniform metadata capturing.

**Metadata Standard**

The Treasury Board Metadata Standard outlines standards and specifications for government institutions to apply to metadata.\(^{54}\) The purpose of the standard is to provide clarity and guidance around information management and information technologies for metadata to encourage ‘the consistent creation, capture and use of metadata ... to manage information as a strategic asset by supporting the capture, description, retrieval, use, re-use, accessibility, sharing, authenticity, reliability, integrity, and maintenance of information resources to facilitate decision-making, accountability, and the efficient delivery of Government programs and services’.\(^{55}\) This in turn is said to promote interoperability across government systems. In theory, such standardisation should facilitate data analytics inclusive of Big Data: first, because there is recognition that collection of metadata has value and therefore should be kept; and second, because there is recognition that a standard in the area facilitates the effective use of metadata to support government operations.

**Summary and Implications**

| Canada does not distinguish between government-held data, open source data, privately-held data and data held by foreign governments. Canada distinguishes instead by the type of organisation holding the data: government, private, or foreign government.  

Federal government agencies access and control measures are derived from three main sources: the Privacy Act, SCISA and Treasury Board Guidelines and Directives. Law enforcement and intelligence agencies (RCMP, CSIS and CSE) are bound by the Privacy Act and SCISA, while the Treasury Board Guidelines and Directives are only meant to provide guidance in various areas around information technology, privacy, and data systems and practices. Treasury Board Guidelines and Directives are not legally binding instruments.  

The Privacy Act imposes some (albeit few) requirements on agency collection and disclosure of data but is not as comprehensive as the Australian Privacy Principles or (as will be explored below) the federal private sector privacy principles in PIPEDA. The purpose of the Privacy Act is to provide an avenue for an individual to ascertain what and how the government collects information about them. The focus is not on providing a comprehensive set of principles for privacy practice amongst Federal government agencies. The Privacy Act of 1983 has not been amended since it entered into force. It is silent on data mining, data analytics, de-identification and, as was seen in the interviews in Chapter 2, is viewed as outdated in the context of protecting privacy in an era of technical advancements. There are no prohibitions on disclosure of data (personal information) to a third party for research or statistics if it is required for the purpose. The assumption is that where personal information is de-identified is may be disclosed and used by other agencies. |

---


\(^{55}\) Ibid.
SCISA does not establish limits and rules around the collection, use and disclosure of information between government agencies (those listed in the legislation including law enforcement, intelligence agencies and other agencies connected to ‘national threat’). The purpose of the Act is to encourage and facilitate sharing amongst designated agencies. It also does not mandate that agencies share information with one another.

The Treasury Board guidelines and directives provide some guidance on data practices but these are not binding on government agencies. The Web Analytics guidelines suggests de-identification of personal information, and provides guidance on disclosure of data to third parties. Disclosure should be pre-authorised, and data should be destroyed 18 months after it is received. As seen in Canada (Information Commissioner) v. Canada (Commissioner of The Royal Canadian Mounted Police), courts view Treasury Board documents are persuasive only when interpreting information obligations.

Warrants are required for federal agencies to intercept private communications as specified in the Canadian criminal code. The courts in Jarvis, Wakeling, Spencer, Telus and Roger provide additional elements of appropriate warrants around data access, use and disclosure.

The legislation and regulatory framework does not refer to data held by foreign governments. Only data about Canadians or those located in Canada was dealt with in the regulatory framework which required data about Canadians be de-identified when given to foreign governments. In addition to this, the O’Connor Recommendations required caveats be placed when identifiable data was given to foreign governments such as stating which institutions are entitled to access the information, as well as procedures should any changes be permitted to how and whom the information is shared with.

3.1.2 Private organisations

Data practice for private organisations is governed under Federal and Provincial privacy legislation based on the principles espoused in Personal Information Privacy and Electronic Documents Act (‘PIPEDA’). Contrary to the Privacy Act, PIPEDA has been amended several times since it was enacted in order to better ensure that privacy protections operate effectively in an evolving technological context. Private organisations have stronger, better and clearer requirements for data access and controls. These are by and large similar to the controls found in Australia around data principles.

Unlike the Privacy Act, PIPEDA contains obligations around data protection, destruction and security. The notion of consent in PIPEDA is more robust and suited to the era of Big Data. Consider the valid consent principle in s 6.1 below:

the consent of an individual is only valid if it is reasonable to expect that an individual to whom the organization’s activities are directed would understand the nature, purpose and consequences of the collection, use or disclosure of the personal information to which they are consenting.

This principle as requires that an individual understand the nature of what they are consenting to, which brings into the array of discrepancies around comprehension of Big Data practices and tools. Big Data is inherently complex. It will be difficult for every day users who are not in this space to comprehend what they are consenting to. There is no guidance globally as to how best to deal with informed consent (assuming it is even

56 Canada (Information Commissioner) v. Canada (Commissioner of the Royal Canadian Mounted Police) [2003] 1 SCR 66.
57 Personal Information Privacy and Electronic Documents Act, S.C. 2000, c. 5.
possible) with Big Data analytics.

Ministerial Authorisations govern metadata practices allowing exchange of metadata between Canada Post and various government agencies. Ministerial Authorisations are not publicly available unless the involved organisations choose to disclose the agreements.

Canada Post is not subject to sharing powers under SCISA but as the primary owner of important national datasets, the organisation is often asked to provide data to those agencies identified in SCISA. Individual Memorandums of Understanding with these departments and agencies have been undertaken, as well as MoUs with agencies and departments not identified in SCISA.

Summary and Implications

Federal private organisations are governed by PIPEDA. The privacy principles identified in PIPEDA are similar to the Australian Privacy Principles. These include, for example, informed consent, security principles, and destruction and retention principles. Crown corporations such as Canada Post are bound by the provisions of PIPEDA. Memoranda of understandings are written for sharing information between federal private organisations. Ministerial Authorisations govern metadata practices including sharing between federal private organisations and government agencies.

3.1.3 Intelligence agencies

Proportional controls on domestic intelligence under the Canadian Security Intelligence Service Act and similar report and policies (CSIS)

The Canadian Security Intelligence Service Act regulates CSIS.58 CSIS is focused on intelligence within Canada, while CSE is focused on foreign intelligence. CSIS may take measures within or outside of Canada to reduce a threat providing that the ‘measures shall be reasonable and proportional in the circumstances, having regard to the nature of the threat, the nature of the measures and the reasonable availability of other means to reduce the threat.’59

CSIS requires a warrant to perform surveillance functions. Such warrants are governed by a special court made of up fourteen Federal Court judges.60 According to the Anderson Report (the Anderson Report is analysed in detail in the UK Report), where some of these judges were interviewed:

They largely hear warrant applications alone but may sit in larger numbers to hear an application and to hear submissions from CSIS on a topic of wider interest, although in such cases the substantive decision is still taken by a single presiding judge. They are entitled to appoint an amicus advocate to make submissions in respect of the privacy issues raised by the application. I was told, in the course of my meeting with several judges of the Court, that they frequently appoint amicus counsel when novel warrants are sought that deploy new technology or propose new applications of old technology. The members of the Court were of the view that those counsel provided them with real assistance. I was told that warrant applicants can be made, heard and determined within 24 hours, and dealt with even faster in an emergency.60

58 Canadian Security Intelligence Service Act, R.S.C., 1985, c. C-23.
59 Ibid, s 12.1(2).
As will be seen in sections 3.6-3.8 of this report, CSIS is subject to an oversight committee, known as the ‘SIRC’, which is composed of Privy Council members. The Committee does not oversee the warrant process, and they only meet a few times per year in their capacity as an oversight body. The Committee can make recommendations only; these recommendations are not legally enforceable.61

In Canada CSIS is subject to the Charter of Human Rights. Section 12.1(3) states:

the Service shall not take measures to reduce a threat to the security of Canada if those measures will contravene a right or freedom guaranteed by the Canadian Charter of Rights and Freedoms or will be contrary to other Canadian law, unless the Service is authorized to take them by a warrant issued under section 21.1.

Section 16 of the Security and Intelligence Service Act provides an exception for CSIS to collect intelligence about a foreign state or foreigner as long as it does not involve Canadian citizens, permanent residents, corporations and is done in Canada.

Canadian law, both legislatively and in case law, takes a stringent view on warrants being required where intelligence leads to an investigation where criminal charges are laid. Whether Big Data is considered reasonable and proportionate will depend on the specifics of the tool, how it is used, and what functions have been built into the algorithms at question (such as de-identification), along with their use.

The Office of the Privacy Commissioner of Canada62 recommended specific amendments for the Privacy Act and PIPEDA. The first recommendation is to curtail over-collection and to have better controls around disclosure. The Report recommended that information only be collected if it is required. It recommended that information exchange with foreign entities have tight controls with caveats, and clarity on what the other entity may do with the data (similar to the O’Connor Recommendations). Intelligence from foreign sources should be internally validated to ensure its accuracy and relevancy. There should be grounds for recourse. Profiling people is discouraged (discrimination). Privacy Impact Assessments should be mandatory. These are all mechanisms of control which currently are not required. Lastly, the Report recommended that there should be regulations to access to open-source information and investigations exploiting publicly available personal information sources. The Report states:

Develop specific guidelines for collection, use and dissemination of intelligence products built upon use of online sources and social network sites. The position of the OPC is that the public availability of personal information on the Internet does not render personal information non-personal. It is our view that departments should not access personal information on social media sites unless they can demonstrate a direct correlation to legitimate government business.63

61 Canadian Security Intelligence Service Act, R.S.C., 1985, c. C-23, s 52.
62 The Office of the Privacy Commissioner of Canada reviewed the checks and controls for the intelligence community and made a number of recommendations around improving privacy and oversight in its Special Report to Parliament – Checks and Controls: Reinforcing Privacy Protection and Oversight for the Canadian Intelligence Community in an Era of Cyber-Surveillance (2014) (the ‘Report’). The Privacy Commissioner recommended a number of revisions to improve transparency, accountability and oversight. These will be discussed later.

(cont.)
The mention of open-source intelligence and the need for regulation is important given how many Big Data systems rely on open-source data. To date, none of the recommendations in the Report relevant to Big Data have been implemented by the Government.

The Report by the Security Intelligence Review Committee\(^64\) highlights a few issues relevant to intelligence agencies’ use of Big Data.\(^65\) The Committee’s 2014-2015 Report identified two aspects relevant for Big Data analytics. CSIS requires a warrant to use and retain metadata about Canadian citizens. SIRC generally reports how many warrants were issued in relation to metadata. In theory SIRC is an oversight body that provides structure and guidance to CSIS but there is no legal obligation on CSIS to provide details of investigations and there have been incidences, as will be examined further in section 3.6, where only partial information has been given to SIRC.

The extent to which meta-data flows between nations in the form of bulk datasets which are analysed abroad presents interesting issues. CSIS is not allowed to access meta-data or other data of a Canadian without a warrant, but this data is able to flow between countries without a warrant provided that the meta-data is de-identified. No matter what precautions are taken to de-identify and thereby find a technical solution, re-identification by the foreign agency remains technically possible. This calls into question whether de-identification of data-sets is a sufficient privacy mechanism when sharing data between borders.

**Proportional controls on foreign intelligence gathering and similar report and policies (CSE)**

The CSE is governed under the *National Defence Act* (NDA)\(^66\) and is subject to Ministerial Directives. These Directives are not publicly available. CSE is a signals intelligence agency and is not mandated to intercept signals of Canadians or people in Canada. Instead its mandate is defined under section 273.64(1) of the NDA:

- (a) to acquire and use information from the global information infrastructure for the purpose of providing foreign intelligence, in accordance with Government of Canada intelligence priorities;
- (b) to provide advice, guidance and services to help ensure the protection of electronic information and of information infrastructures of importance to the Government of Canada; and
- (c) to provide technical and operational assistance to federal law enforcement and security agencies in the performance of their lawful duties.

After the terrorism incidents on September 11, 2001 the Canadian government introduced the *Anti-Terrorism Act 2001*. When that Act came into force it added Part V.1 to the NDA, which set out CSE’s three-part mandate.\(^67\)

---

\(^64\) The primary role of CSIS is to perform domestic intelligence over people in Canada. They are overseen by the Security Intelligence Review Committee. Every year, the independent SIRC meets with CSIS to go over operations, and delivers a report to Parliament.  
part (a) authorizes CSE to acquire and use foreign signals intelligence in accordance with the Government of Canada’s intelligence priorities;

part (b) authorizes CSE to help protect electronic information and information infrastructures of importance to the Government of Canada; and

part (c) authorizes CSE to provide technical and operational assistance to federal law enforcement and security agencies, including helping them obtain and understand communications collected under those agencies’ own lawful authorities.

CSE is bound by s 8 of the Privacy Act, requiring them to protect the privacy of Canadians. That obligation is further strengthened in s 273.64(2) of the NDA titled ‘Protection of Canadians’. That section states:

(2) Activities carried out under paragraphs (1)(a) and (b)

(a) shall not be directed at Canadians or any person in Canada; and

(b) shall be subject to measures to protect the privacy of Canadians in the use and retention of intercepted information.

They may not directly collect intelligence on Canadian citizens or people in Canada. CSE may, however, provide assistance to federal law enforcement and security services (RCMP and CSIS) but only under the condition of lawful authority requiring the RCMP and/or CSIS to have a warrant or court order.

It is not possible for CSE to collect foreign intelligence without incidentally sweeping some ‘private communications’.\(^{68}\) \(^{69}\) There is a special authorisation regime under the NDA involving the Minister of Defence to serve as an agent of oversight for these inevitable and incidental sweeping of private communications. Without this mechanism CSE would be in breach of the Criminal Code Part VI where unlawful interceptions are prohibited.\(^{70}\) This means that CSE is not subject to the courts in requiring a warrant to lawfully intercept signals even when incidental private communications of Canadians are intercepted.

See 3.6 for issues of oversight and accountability.

Reasonable and Proportionate in Canadian Law

As seen in the previous sections, the courts, legislative provisions (in particular the Charter of Human Rights and Freedoms) and various reports all emphasise that practices limiting rights and freedoms must be reasonable and proportionate. This is measured against what the practice or provision hoped to achieve.

Legislative measures refer to reasonable and proportionate aspects, for example the Canadian Security Intelligence Service Act allows CSIS to take measures within or outside of Canada to reduce a threat provided that the ‘the measures shall be reasonable and proportional in the circumstances, having regard to the nature of the threat, the nature of the measures and the reasonable availability of other means to reduce the threat.’\(^{71}\)

The Charter of Human Rights and Freedoms is part of the Canadian Constitution and applies to all government actions. As such, governments should consider the Charter before taking any actions that would otherwise interfere with human rights and freedoms. Human rights

---

\(^{68}\) Section 273.61 of the National Defence Act states that ‘private communication’ has the same meaning as in section 183 of the Criminal Code.

\(^{69}\) Criminal Code, R.S.C. 1985, c. C-46, ss 184(1) and 184(2).


\(^{71}\) Canadian Security Intelligence Service Act, R.S.C., 1985, c. C-23, s 12.1(2).
and freedoms are not, however, absolute. Section 1 of the Charter acts as a safeguard against legislative provisions which violate human rights:

1. The Canadian Charter of Rights and Freedoms 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.

Under this section, for example, provincial and federal governments may limit rights and freedoms, but only if they can demonstrate that the law or policy is set out in law, pursues an important goal which can be justified in a free and democratic society, and pursues that goal in a reasonable and proportionate manner.

The reports and recommendations previously examined, such as in the O’Connor Recommendations, also refer to reasonableness and proportionality.

Also noteworthy is the fact that the intelligence agencies do not consider themselves bound to comply with Federal Court decisions as articulated in X (Re)\(^2\) or at least only the aspects of a decision the organisation itself deems appropriate to its mission. The CSE is subject to review by the Minister of Defence, recommendations by the Commissioner, and to Ministerial Directives yet there are no direct legal consequences for not meeting requirements set by the courts. It is hard to reconcile reasonable, necessary and proportionate in what could be seen as a somewhat self-regulated sphere, insufficient oversight or a system that lacks sufficient transparency.

**Summary and Implications**

The Canadian position on controls of data, and in particular controls around privacy, is significantly more complex than the principle based approach in Australia. Federal government agencies must adhere to the Privacy Act 1983. The Act has not been amended since 1983 and is ill-equipped to deal with many issues that arise in the context of technology. This must be contrasted to PIPEDA which governs private organisations, is principle based and has been amended on numerous occasions in order to accommodate privacy concerns generated by the use of new technologies.

Intelligence agencies such as CSIS and CSE follow Ministerial Guidelines on privacy and information disclosure. Warrants are required by CSIS to obtain information about a Canadian or person in Canada. The situation outside of Canada is less clear as is the requirements of data exchange between foreign agencies.

In theory any bulk datasets flowing across border such as meta-data must be de-identified. There are no rules on re-identification once the data crosses borders. When information is exchanged across borders it is often now done with caveats (post O’Connor Recommendations) but such caveats discuss limits on third party disclosures and not re-identification or what type of analytics is allowed to be run on data sets. Re-identification in Canada is not clear cut but the Supreme Courts’ decisions in Wakeling, Jarvis and Spencer indicate that where there is an expectation of privacy any use of data for an investigation leading to criminal charges will require a warrant. It is likely that a warrant will be required down the road for re-identification performed by agencies within Canada.

---

\(^2\) X (Re) (2013) FC 1275.
3.2  Are legal controls comprehensive and proportional?
See 3.1.

3.3  Are legal rules clear, principle-based, consistent and instructive?

The third lens principle looks at some of the attributes in the Canadian regulations and policy framework around data, data sharing, and national security. We consider whether the framework is expressed in clear, principle-based and consistent legal rules that provide officials with appropriate guidance to take reasonable decisions and perform their functions correctly and efficiently in a dynamic environment.

There are three general consistent principles that are expressed at many points in the legislation, policies and case law. These three principles are:
- that practices, guidelines and provisions be reasonable and proportionate;
- the requirement of ‘legal authority’ for investigations; and
- that there are framework of compliance audits

3.3.1 Reasonable and proportionate

The notion of ‘reasonable and proportionate’ for the Lens refers to clear principles-based drafting and not the Charter of Human Rights and Freedom concept of whether a legislative provision restricts a right or freedom in a manner that is ‘reasonable and proportionate’.

The principles elaborated in the Privacy Act are clear and principle based but are so out of date as to render them of limited value when applied to Big Data and any technology developed post-1983 including the Internet.

Treasury Board documents relevant to the space are equally clear, principle-based and are additionally quite flexible. Government agencies are free to adopt principles as best suits their organisation. Unfortunately, however, clear and principle based does not necessarily equal adequate. The flexibility in these Guidelines and Directives often means that best practices are not used, and assumes that agencies will be able to keep on top of emerging issues, and alter their practices in accordance with the principles.

3.3.2 Legal authority for investigations

As previously outlined in Section 3 of this Report the Canadian courts have consistently insisted on legal authority such as a warrant to access and use data in the course of an investigation. The trilogy of the cases Spencer, Jarvis and Wakeling suggest that the courts take a consistent approach to the infringement of Articles 7 and 8 of the Charter, requiring legal authority to access and use data in the course of an investigation.

3.3.3 Framework for compliance audits

Canadian government departments are subject to regular, ongoing compliance audits. These are performed for three different reasons. The first, legislation and regulations may require compliance reviews. Second, audits are a form of risk management and assessments that organisations often undertake. And third, if the Treasury Board feels that a department is not compliant with a particular policy or directive they may order an audit.

3.3.4 No publicly available guidelines on Big Data, data analytics, or bulk data-sets

There are no direct guidelines or directives on Big Data, bulk data-sets or data analytics that are publically available. Ministerial Directives may provide guidance the intelligence
agencies but these are secret documents and therefore unavailable for assessment. The Web Analytics Standard addresses aspects of the collection of Cookies and collection of information on the use of Government websites.

3.3.5 Treasury Board Metadata Standards

The Metadata Standards set by the Treasury Board establish a basic standard to make metadata capturing harmonised amongst government agencies. It does not deal with guidelines around collection, use, or disclosure.

3.3.6 Treasury Board policies and directives

The courts have on numerous occasions unequivocally stated that such policies and directives are binding with regards to employment laws, pensions and contractual agreements and the like. Other areas such as privacy related guidelines can be seen as soft law, or as providing guidance in interpreting legislation but the policies themselves are not binding. Additionally the organisation may decide to bind itself to such policies in a more substantial manner – the policies themselves, however, are largely general principles so there is great leeway in how an organisation implements such policies.

There is only one decision involving Treasury Board Guidelines or Directives outside the scope of employment. The decision Canada (Information Commissioner) v. Canada (Commissioner of The Royal Canadian Mounted Police) addressed the issue as to whether the Court should turn to the Treasury Board for guidance in interpreting s 3 of the Privacy Act, and s 19 of the Information Act and in particular, look to the Treasury Board Manual on Access to Information. It was held that Manuals are to be given less weight in evaluating legislative instruments. The court further noted that Guidelines and Directives, however, would be given more weight than mere manuals for interpreting privacy principles, but the court did not go into detail in terms of how binding or how influential Treasury board Guidelines and Directives may be in this sphere.

There are many other Treasury Board Guidelines and Directives (over 30) that have one or two elements that may indirectly and remotely relate to data but they are sufficiently removed from the subject so as to cloud the Canadian position on Big Data. The dense, complex and piece-meal nature of the Canadian context makes the ascertainment of the principles behind data use uncertain, and difficult to implement, especially in a time-limited critical situation.

---

74 X (Re) (2013) FC 1275.
Summary and Implications

The Canadian framework strives for clarity and transparency yet examination of the various polices, directives and legislation does not provide a clear picture for many data practices.

The Treasury Board documents are non-binding. The Privacy Act provisions are out-of-date and are not principle based. A focus on privacy principles and standards in data practices is required to ensure consistency while maintaining flexibility across contexts. While the Treasury Board documents are both flexible and principle based they are merely persuasive. In an area that directly impacts on rights and freedoms guaranteed under the Charter binding legislative provisions seem more appropriate than mere guidelines. Additionally, there are no Treasury Board guidelines and directives looking at more advanced data analytics (reference to Web analytics such as cookies).

3.4 Is integrity of data and analysis supported?

The fourth line of enquiry addresses the need for data quality and integrity as well the integrity of the inferences drawn from data through analysis and employed in decision-taking. This section considers current rules that would support the integrity of data collected, retained and accessed by government for law enforcement and national security purposes, and the integrity of analytical and decision-making uses of such data and systems.

There is little by way of direct, public data integrity requirements for decision-making.

The O'Connor Recommendations address data integrity in the context of sharing data with foreign agencies. Recommendation 8 states:

Mandatory screen for relevance, reliability and accuracy of information to be shared with other agencies in accordance with relevant laws respecting personal information and human rights.

Curiously, the Privacy Act 1985 does not refer to notions of reliability, accuracy, authenticity, integrity or security of data.

Enabling legislation such as the National Defence Act and the Royal Canadian Mounted Police Act also do not refer to reliability, accuracy, authenticity, integrity or security of data.

PIPEDA refers to principle of accuracy of data, but law enforcement and intelligence agencies are not bound by PIPEDA though private organisations such as Canada Post are bound by the principles.75 Principle 6 requires that:76

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

Accuracy is required when personal information is disclosed to third parties. To this purpose, organisations must strive to ‘minimize the possibility that inappropriate information may be used to make a decision about the individual’.77

Data integrity and quality is important for making informed decisions. The Treasury Board may provide relevant guidelines and directives in this area which help to guide agencies in establishing data control frameworks, particularly data integrity and quality frameworks. The
agencies and departments themselves, however, are responsible for establishing their own internal frameworks and processes.\textsuperscript{78}

In our review of Treasury Board guidelines and policies we were unable to find any general principles requiring data accuracy as a stand-alone principle such as those found in PIPEDA with one exception, Privacy and Data Protection Guidelines – Employee Privacy Code.\textsuperscript{79} This Guideline contains several privacy principles similar to PIPEDA including the duty to maintain accurate datasets on employees. This Guideline has been archived. According to the Treasury Board website:

\begin{quote}
Information identified as archived is provided for reference, research or recordkeeping purposes. It is not subject to the Government of Canada Web Standards and has not been altered or updated since it was archived. Please contact us to request a format other than those available.\textsuperscript{80}
\end{quote}

In the context of information technology policy, however, there is a general security principle that incorporates integrity. The Treasury Board Policy Framework for Information Technology states:

\begin{quote}
Ensuring the confidentiality, integrity, and availability of information is essential to government decision-making and the delivery of services. Effective security of information requires a systematic approach that identifies and categorizes information and associated assets, assesses risks to them, and implements appropriate personnel, physical, and IT safeguards.\textsuperscript{81}
\end{quote}

There is a similar clause in the Operational Security Standard: Management of Information Technology Security (MITS) which applies the general principle that the more important the asset, the greater the risk therefore requiring appropriate controls including integrity of information.\textsuperscript{82} How an agency implements the standard, however, is left to them to choose.

There is no further development of this concept in Treasury Board documents.

**Summary and Implications**

Data integrity is regulated in the federal private sector in Canada but not in the public sector. Relevant documents addressing data integrity issues are non-binding Treasury Board documents related to information technology. There is no general data integrity principle in either the Privacy Act or in the privacy related guidelines from the Treasury Board. The exception is privacy in employment context where data integrity is required; this is likely because employment is the only area where Treasury Board Guidelines and Directives are binding legal instruments (as discussed in 3.1 and 3.2).


\textsuperscript{80} Ibid.


Big Data tools and culture are well known for their capacity to accept data which is less reliable, complete, accurate, up to date or relevant than usually required for data systems. But while the tools may deliver output from low integrity input or unverifiable assumptions, and preserving provenance may allow for humans to give less weight to poor quality data, the integrity of the outcome remains uncertain until the Big Data system is fully implemented and regularly tested.

Law enforcement processes producing criminal evidence is guided by the rigour that accompanies testing in an adversarial, open court process with strict rules of admissibility, relevance and probative value.\(^3\) Criminal and national intelligence processes, on the other hand, necessarily rely on less rigorously tested and verified information. As is appropriate to the nature of their task, accepted standards of ‘proof’ or probative value are typically below the standard of ‘beyond reasonable doubt’. In addition, these processes are often necessarily secret and citizens who may suffer negative consequences as a result of incorrect data do not have the opportunity to challenge or correct the data. While this is a necessary feature of the terrain, and of necessity less reliable information has to be utilised, the use of Big Data models for decisions which have impacts on individuals without the rigorous testing of a court process raise questions about how to set the appropriate standards and expectations of integrity, probative value and relevance.

Intelligence analysts are skilled to deal with data that has differing levels of integrity. Action may be taken on lower quality data where a significant national security breach may be pending. Where, however, there is a less compelling or serious harm involved, making decisions affecting individuals on lower quality information may be disproportionately adverse.\(^4\)

Legal rules do not currently regulate such intelligence decisions but clearer rules may be required for Big Data systems to ensure that uncertainty is preserved so the inferences/predictions can be given estimates of truth in line with the provenance of the underlying data. This may be consistent with the current rules (which are beyond the scope of the report).

Big Data tools, more than other intelligence methods, may be used in situations far removed from the source of the information on which they depend, the knowledge of those with actual experience of the source, and the consequences of decisions which they may suggest. One important aspect of integrity is to ensure that appropriate efforts are made to consider the logical and inferential reliability of the output as a basis for making decisions about individuals.

\(^3\) There are extensive provisions about information use in Evidence Acts, Rules of Court, case law and other laws.

\(^4\) This is an area where discussion of scope creep is relevant: acceptance of the need to use lower quality data in ‘extreme’ cases may lead to such use in less ‘extreme’ cases.
As noted in the literature review in chapter 2 of the Methodology Report, Big Data analytics, especially prediction of intrinsically uncertain future events, are typically based on statistical or algorithmic correlation, but legal consequences and the notion of responsibility is more often tied to causation. This potential divergence between analytical methods and a requirement of being able to attribute causal responsibility may restrain inappropriate interpretation of correlation. This is in particular so in cases where a decision could only be justified on the ground that causality is demonstrated (either because an individual is affected, or because it is assumed that a policy change will have a particular impact). No comprehensive provisions in statutory or other rules or controls specifically address this problem.

3.5 Are data and systems protected?

The fifth line of enquiry considers the rules which protect the security of relevant data and systems. There are three pieces of legislation that address the security of data and systems. There are only relevant provisions binding private organisations (PIPEDA, Data Breach Notification). There are no binding security provisions for law enforcement and intelligence agencies.

3.5.1 Safeguarding data (security provision)

Safeguarding security is principle 4.7 (Safeguards) of PIPEDA. PIPEDA is only binding on private organisations and not on government agencies.

Principle 4.7 stipulates the following safeguards:

- The security safeguards shall protect personal information against loss or theft, as well as unauthorized access, disclosure, copying, use, or modification (s 4.7.1)
- Information should be protected on a sliding scale. The more sensitive the information the higher levels of protection that are required (s 4.7.2)
- Protections measures should include in s 4.7.3(a-c):
  - Physical measures, for example, locked filing cabinets and restricted access to offices;
  - organisational measures, for example, security clearances and limiting access on a ‘need-to-know’ basis; and
  - Technological measures, for example, the use of passwords and encryption.
- Employee awareness of personal information confidentiality is important (s 4.7.4)
- When disposing of personal information care should be taken to prevent unauthorised parties from accessing the information (s 4.7.5)

There are no equivalent safeguarding obligations in the Privacy Act which binds government organisations.

3.5.2 Data breach notification

The Digital Privacy Act 2015 was passed on June 18, 2015 which amended aspects of the Personal Information Protection and Electronic Documents Act (PIPEDA) and entered into force also on June 18, 2015. One of the amendments was to introduce new data breach notification law into PIPEDA. Private organisations must now report security breaches involving personal information to the Privacy Commissioner. There are the requirements for data breach notification85:

85 Section 10.1 PIPEDA sets out the requirements
• The personal information must be under the organisation’s control
• Reasonable real risk of significant harm to an individual
• Significant harm is not defined
• Organisation makes determination if there is a real risk of significant harm
• Where there has been a breach individuals need to be notified
• If organisation doesn’t notify they may be fined $100,000 CND per breach.

In 2014 The Treasury Board chanced the Directive on Privacy Practices whereby the federal public sector is encouraged to report data breaches to the Treasury Board Secretariat, the Office of the Privacy Commissioner, and to notify those individuals whose personal information has been breached. Similar to the amendments of PIPEDA the breach notifications have a risk-based standard of serious harm. Again, Treasury Board documents are not binding on federal government agencies while the agencies themselves determine what constitutes ‘serious harm’. As revealed in tables reported to Parliament and published in Canadian newspapers, the number of breaches that occurred did not equate to number of breaches reported in 2015. For example, the Canadian Revenue Agency had 3868 breaches with 26 reported. The RCMP had 52 breaches with 25 reported. CSE had 13 breaches with none reported. Curiously, CSIS had only 1 breach and reported only one breach. The Office of the Privacy Commissioner is investigating CSIS in this matter.

3.5.3 Computer offences

The Canadian Criminal Code criminalises various actions related to hacking. Section 34.2.1 provides:

342.1(a) 1 Everyone who, fraudulently and without colour of right,
   (a) obtains, directly or indirectly, any computer service,
   (b) by means of an electro-magnet, acoustic, mechanical or other device, intercepts or causes to be intercepted, directly or indirectly, any function of a computer system,
   (c) uses or causes to be used, directly or indirectly a computer system with intent to commit an offence under paragraph (a) or (b) or an offence under section 430 in relation to data or a computer system, or
   (d) uses, possess, traffics in or permits another person to have access to a computer password that would enable a person to commit an offence under paragraph (a), (b), or (c)

is guilty of an indictable offence and liable to imprisonment for a term not exceeding ten years, or is guilty of an offence punishable on summary conviction.

Section 430 criminalises a number of actions related to data mischief from destroying and altering data; rendering data meaningless or ineffective; obstruction or interruption or interference with lawful use of data or any person who are using the data lawfully or those who are entitled to have access to the data.

---

86 Section 28 PIPEDA.
3.5.4 Treasury Board policies and directives

The following represent the most relevant documents on security of data and systems:

- Operational Security: Management of Information Technology Security Standard
- Government Security Policy

**Operational Security: Management of Information Technology Security Standard**

This Treasury Board Standard is tri-partite. Part I contains general information about information technology security. Part II addresses management and organisational aspects of information technology security within departments. Part III provides technical and operational safeguards.

Part II requires that there be designated positions with the department for security personnel such as Chief Information Officer, Business Continuity Plan Coordinator, IT Security Coordinator, Departmental Security Officer, Operational Staff, and a COMSEC Custodian who is responsible for classified and encrypted data. Each department is required to have an Information Technology Security Policy, and to perform risk management of security concerns on a continual basis. This includes internal audits, training on an ongoing basis, security awareness, vulnerability assessment, written agreements where information or infrastructure is shared between departments or with other organisations, and similar IT security aspects (s 12 of the Standard).

Part III requires all departments to have graduated safeguards whereby appropriate controls around accuracy, integrity, confidentiality and availability are commensurate with the risks and assets. It is assumed under s 13 that Departments will segregate sensitive information in order to provide better safeguards to reduce security costs. All departments are required to have an active defence strategy that stresses prevention, detection, response and recovery (PDRR) with emphasis on prevention (s 15). Security preparedness requires ongoing monitoring and close communication with Public Safety and Emergency Preparedness Canada (PSEPC) which provides alerts and advisories. Such Safeguards are meant to guard against a cyber security attack. Section 16 is the most relevant aspect to Big Data.

Section 16 is focused on Prevention Safeguards to protect the confidentiality, integrity, and availability of information and IT assets. Section 16 addresses:

- Physical security
- Storage, disposal and destruction of information
- Personnel security in the IT security environment
- Technical safeguards including: selection of
  - Security products (16.4.1),
  - Identification and authentication (16.4.2),
  - Authorization and access control (16.4.3),
  - Cryptography (16.4.4),
  - Public key infrastructure (16.4.5),
  - Network security and perimeter defence (16.4.6),
  - Mobile computing and teleworking (16.4.7),
  - Wireless devices (16.4.8),
  - Emanations security (16.4.9),
  - Telecommunications cabling (16.4.10),
  - Software integrity and security configuration (16.4.11), and
  - Malicious code.
Part III further elaborates on detection, response, recovery and so forth, and is comprehensive. Again, the standard reflects a graduated safeguards approach to protecting and securing information and assets. Privacy is not referred to in this document though in other policies and guidelines both privacy and security aspects are included. For example, in the guideline, ‘Taking Privacy Into Account Before Making Contractual Decisions Guidance Document’ the same elements are listed as found in the Security Standard but technological safeguarding measures refer to enhancing both privacy and security, and both must be assessed in internal audits.

**Government Security Policy**

The Government Security Policy issues by the Treasury Board are a document directed to Deputy Heads of Departments outlining an accountability framework for matters of government security. The Policy, however, is focused more around security clearances and matters of security breaches from personnel. While protecting data / information is part of the Policy, it is not at the forefront.

The Treasury Board Secretariat according to s 7 of the Government Security Policy may require an audit, and make remedial recommendations and take corrective action.

**Summary and Implications**

Security safeguard mechanisms for federal government agencies are similar to privacy mechanisms. There is little by way of binding legislative provisions to ensure that data is secure. There are many different Treasury Board documents such as data breach notification ‘Directive on Privacy Practices’ and ‘Government Security Policy’ but these are not binding. This discretion on whether to report data breaches is seen in the empirics where CSIS only allegedly had one breach which was reported. The RCMP reported half of their breaches. While the CSE had breaches they did not elect to report any. This potential under-reporting has led the Privacy Commissioner, Daniel Therrien, to launch an investigation into CSIS’s breach reporting.

This is to be contrasted with the federal private sector’s obligations to keep data secure under PIPEDA. PIPEDA also includes data breach notification law with the Office of the Privacy Commissioner where fines of up to $100,000 may be imposed for non-compliance.

### 3.6 Is accountability maintained?

The sixth lens addresses appropriate oversight which is inclusive of governance issues and accountability. The framework would ensure that access to data and data analysis and use for decisions is tracked and audited for justification, security and intrusiveness, and that decisions are subject to appropriate internal governance as well as independent oversight and accountability. Decision-makers should remain accountable for their decisions, which imply an understanding of the provenance and integrity of data and awareness of any biases in the analytic process. As will be seen below, oversight remains a concern for the RCMP, CSIS, CSE and the lack of oversight for agencies sharing data under SCISA.

#### 3.6.1 The role of the Treasury Board Secretariat

The Treasury Board Secretariat provides oversight on the management of the public service programs through the Managing Accountability Framework (MAF). MAF enables Deputy Heads of Departments to provide evidence that they are complying with Treasury Board Directives and Policies. If the TBS is unclear or unsatisfied of compliance or if they believe...
there are inefficiencies they may request than the Deputy Head arrange for an internal audit and that this audit be shared with TBS. Recommendations may be made following an internal audit. It is unknown if the RCMP, CSIS and CSE are subject to this framework. The oversight and accountability mechanisms are discussed below.

3.6.2 RCMP (National Law Enforcement)

The Federal Court, the Civilian Review and Complaints Commission, and the Royal Canadian Mounted Police External Review Committee provide oversight for the RCMP.

The Royal Canadian Mounted Police External Review Committee (PERC) is an administrative tribunal that deals with decisions made requiring review around employment and carrying out of duties. According to its website the PERC may review decisions:

- to dismiss or to demote an RCMP member, or to impose a financial penalty of more than one day's pay, for contravention of the RCMP Code of Conduct;
- in a harassment complaint investigation;
- to discharge or to demote a member for being absent from duty; and
- to stop a member’s pay and allowances when the member has been suspended from duty

This oversight is not directly relevant to Big Data.

The Civilian Review and Complaints Commission for the RCMP (CRCC) were formed in 2014 through the Enhancing Royal Canadian Mounted Police Accountability Act 2014. This Commission reviews complaints made against members of the RCMP. The Commission is an independent agency. There is an internal mechanism where members of the public may issues complaints against the RCMP directly. The CRCC then mainly deals with complaints where an individual is dissatisfied with the outcome of the internal RCMP complaints mechanism. The CRCC submits reports, holds hearings, and makes recommendations to practices and policies.

3.6.3 The courts

The RCMP’s actions are subject to the Federal Court. As previously seen in Chapter 1 and 3.1-3.2 of this chapter, the court has played an important role in overseeing the RCMPs’ investigations. The court has consistently insisted that access and use of data for the purpose of an investigation requires a court order or warrant as per Jarvis, Spencer, Wakeling, Telus and Rogers.

Recent media reporting, access to information requests and a recent court case have raised questions about whether these entities are subject to the Treasury Board policies. After reading enabling legislation, Treasury board policies, and searching for case law on point, it still remained unclear if these entities fell under the jurisdiction of the Treasury Board in terms of policies. Information requests were made to organisations with responses stating that this was unclear.

Mirarchi v. R (2012) QCCS 7087. R v. Mirarchi (2016) QCCA 597. The RCMP may apply to the court in secret to compel technology communication companies to release decryption methods. The media reported for example that the RCMP applied to the Federal Court to intercept and decrypt messages sent through Blackberry Devices between members of the mafia. This was known as ‘Project Clemenza’ which is reportedly running from 2010 and 2012, and is said to have resulted in over 1 million messages being decrypted. The investigation resulted in the case R. v. Mirarchi which involved of investigation of a mafia member being murdered by a rival mafia group.

The RCMP intercepted communications and decrypted messages in the investigation of serious organised crime. The media, however, is interested in the case because the global encryption key

(cont.)
issues about the privacy-invasive use of certain technologies, and the extent and effectiveness of oversight and accountability regarding the collection and use of data by the RCMP.

3.6.4 Security Independent Review Committee (SIRC)

The Security Independent Review Committee (SIRC) has Primary Oversight of CSIS. SIRC is composed of Privy Council members. The Committee does not oversee the warrant process as was seen in s 3.2 of this Report, and they only meet a few times per year in their capacity as an oversight body. The Committee can make recommendations only; these recommendations are not legally enforceable. SIRC produces an Annual Report for Parliament.

Pursuant to s 34 of the SIRC Act the committee has the general duty to review the practices of CSIS and individuals may complain about CSIS to the SIRC. The SIRC may investigate and make recommendations accordingly.

CSIS is in theory subject to the Federal Courts and must adhere to the Canadian Charter of Human Rights. In practice, however, the jurisdiction appears uncertain as will be highlighted below.

Section 12.1(3) of the Canadian Security Intelligence Service Act states:

> The Service shall not take measures to reduce a threat to the security of Canada if those measures will contravene a right or freedom guaranteed by the Canadian Charter of Rights and Freedoms or will be contrary to other Canadian law, unless the Service is authorized to take them by a warrant issued under section 21.1.

The leaks by Edward Snowden, then later the Federal case of involving the confidential court with Judge Mosely (later made public), and an Access to Information request by the Globe and Mail, combined to reveal that CSIS had made requests to CSE (and indirectly the Five

allows anybody’s communications using a Blackberry device to be intercepted and decrypted. This means that having the encryption key allows far greater access than merely to those members of mafia who were the subject of the investigation. Further it remains unknown if the encryption key was handed over after a court order (if so, secret) or voluntarily by Blackberry. As such it is difficult to ascertain if this potential ‘weapon of mass surveillance’ is subject to appropriate safeguards, transparency and accountability.

Another tool used by the RCMP has been the subject of debate in the media, the courts, and now the Officer of the Privacy Commissioner. Earlier in 2015 it was revealed that the RCMP used what is known as an IMSI catcher or as they are commonly referred to, ‘StingRays’. IMSI stands for international mobile subscriber identity which is an internationally standardised unique number consisting of 64-bits to identify a mobile subscriber/cellular device. The media has reported in a leaked correctional services email that IMSI a ‘StingRay-like device was installed in an Ontario prison to monitor inmate communications, but also caught innocent people outside the facility in the dragnet.’ A StingRay type device is ‘a device that can triangulate the course of a cellular signal by acting like a face cell phone tower and measuring the signal strength of an identified device from several locations.’ StingRay type devices sweep up all cellular signals in an area and cannot at this point be limited to the individuals and their devices being investigated.


The Privy Council is the secretariat providing advice to members of the Federal Cabinet.

Canadian Security Intelligence Service Act, R.S.C., 1985, c. C-23, s2.

X (Re) (2013) FC 1275.

(cont.)
Eyes community) to provide data about Canadians to assist them in investigations. This thwarted the privacy protections and warrant requirements. As the *Globe and Mail* news investigation reveals:

In a highly unusual statement, the Federal Court says that Justice Richard Mosley found last week that the Canadian Security Intelligence Service was not sufficiently open about all the surveillance alliances it planned to form. Five years ago, CSIS had persuaded him to sign off on a foundational eavesdropping warrant to extend its reach outside Canada... the court gave a hint of what is coming. ‘Justice Mosley has found that CSIS breached its duty of candour to the Court by not disclosing information that was relevant,’ the statement said. And it added that, despite perceptions to the contrary, ‘the Court considers it necessary to state that the use of ‘the assets of the Five Eyes community’ is not authorized under any warrant issued.’

In addition to the questions regarding the extent to which the CSIS and CSE are subject in practice to the jurisdiction of Canadian Federal Courts, there is also no legal remedy (outside of a Ministerial order) for when practices and powers are questioned as will be explained below.

The Canadian situation is complex. The law prohibits CSIS from accessing data about Canadians without a warrant. Several case studies reveal that agencies are not always abiding by these rules, or they are deliberately leaving out information when presented in front of courts. This is a tense and difficult situation. In theory the law states that CSIS is subject to the authority of the Federal Court. Whether CSIS later complies with direction from the courts or omits information has been the subject of debate in Canada. If the agency’s practices are challenged before the courts, the courts provide direction, that direction may or may not be taken, and there are no obvious enforceable measures that can be taken against the agency, one must question the oversight and accountability mechanisms.

It was revealed further in *X (Re)* by Judge Mosley that both CSIS and the RCMP made requests to CSE to ask Five Eyes allies for intercepted communications of Canadians or permanent resident of Canada living or traveling abroad. This has been interpreted as a method of getting around warrant requirements as CSIS and the RCMP require warrants to intercept communications. CSE does not as they are meant to capture intelligence of


97 For example, in an audit it was accidently revealed that a member of CSIS had requested tax information from Canadian Revenue Agency (CRA) without a warrant. When SIRC reviewed the matter they were told this was an isolated incident. It became apparent during the review, however, that this was not the case and that there had been several incidences of the CRA handing over information to CSIS without a warrant. Once SIRC began to review the incident the requests for data to the CRA were deleted from the CSIS database. The SIRC only has the power to review the incident and make suggestions for future approaches. The SIRC recommended that the Federal Court review the matter and that the Privacy Commissioner have access to such requests. CSIS responded to this request as being inappropriate.

98 *X (Re)* (2013) FC 1275.

(cont.)
foreigners, not Canadians. It became apparent during the course of multiple proceedings that both CSE and CSIS were potentially stretching their power. Judge Mosely writes:

Based on the documentary record before me and Mr. Abbott’s evidence, I am satisfied that a decision was made by CSIS officials in consultation with their legal advisors to strategically omit information in applications for 30-08 warrants about their intention to seek the assistance of the foreign partners. As a result, the Court was led to believe that all of the interception activity would take place in or under the control of Canada.

Judge Mosley’s decision was appealed to the Federal Court of Appeal which upheld the lower court’s decision. The Supreme Court of Canada will hear the appeal. No reasons were given on the Supreme Court’s decision to hear the appeal and no court date has been set.

It remains to be seen if newly enacted SCISA will change practices of information sharing between agencies, and in particular between CSIS and the CSE, as well as with other entities. The court in Jarvis, Spencer and Wakeling has provided a consistent view that warrants are still required for investigations otherwise there is a risk of ss 7 and 8 of the Charter of Human Rights and Freedoms being violated. Charter litigation is expected around SCISA. It is of further interest as to how SCISA will affect future decisions by the Federal Court as to the Agencies’ abilities to access, use and disclose data within Canada. SCISA does not discuss sharing between foreign governments.

As previously stated, the Trudeau Government has announced its intention to review and change oversight for the Canadian security intelligence sectors, but it has not announced what these changes might entail.

3.6.5 The CSE Commissioner

The CSE Commissioner has Primary Oversight of CSE with the Minister of Defence

A Commissioner whose duties are carried out under s 273.63 of the NDA oversees the CSE. The Commissioner tables an Annual Report to Parliament, which reviews the actions of CSE.

The CSE is overseen by a Commissioner (a retired judge) whose duties are carried out under s 273.63 of the National Defence Act. The Commissioner tables an Annual Report to Parliament, which reviews the actions of the CSE. This Report offers recommendations only but is seen as an important oversight mechanism.

After the release of the Commissioner’s Annual Report 2014-2015 the press reported that Canadian’s metadata was being shared by the CSE with foreign intelligence without properly stripping or de-identifying personal information. The Minister of Defence temporarily halted the exchange of information with Five Eyes to ensure that technical means around

99 Ibid, at [116]–[125].
100 Ibid, at [90].
101 Jim Bronskill, ‘Supreme Court to weigh legality of CSIS overseas spying’ (5 February 2015) The Globe and Mail. There is nothing reported on the Supreme Court of Canada’s website relating to this appeal.
metadata of Canadians was protected. In this instance we see the newly elected Minister of Defence swiftly and directly overseeing this violation in a transparent and clear fashion, thereby, exercising his oversight ability in a manner fitting with the lens principle. This is of interest for several reasons.

First, the newly elected Minister of Defence announced the discovery. It is unknown based on the facts if this was a genuine mistake where data was insufficiently de-identified, or whether this was leeway that the organisation was prepared to take under the previous Harper government. The Commissioner, however, did state that the CSE had been forthcoming, were open to fixing the mistake, and that the insufficiency was not deliberate and that the Ministerial orders and legislative provisions were not being deliberately ignored. But he went on further to indicate that CSE had not taken sufficient due diligence in the matter. The Commissioner also stated that the NDA, as noted in previous Annual Reports, required amendments to provide a clearer framework for metadata activities.

Second, as previously highlighted, obfuscating personal information or de-identifying metadata doesn’t prevent re-identification. Even though the Canadian system makes an attempt to de-identify meta-data flowing between partner countries, there is nothing to prevent the other nation from running the meta-data through methods that allow re-identification. This wouldn’t require a warrant and Big Data systems are capable of this.

Third, the metadata information reported in the Annual Report, which it did not reveal in the press, was whether or not bulk datasets (de-identified or otherwise) were being shared with foreign governments. However, the inferences in the Report and in the media give the strong likelihood that this is the case.

3.6.6 No Direct Oversight over Security of Canada Information Sharing Act 2015 (SCISA)

Previously discussed in 3.2, the Security of Canada Information Sharing Act 2015 (SCISA) shields participating government agencies from civil liability arising from information sharing, and creates a framework to encourage information sharing. As seen in the interviews in all three countries, information silos remain a consistent problem amongst government agencies.

SCISA does not mandate information sharing, not even between CSIS, CSE and the RCMP. It merely creates legislation to encourage sharing. Information disclosure as such is allowed ‘in respect of activities that undermine the security of Canada, including in respect of their detection, identification, analysis, prevention, investigation or disruption.’Ironically, information sharing between the agencies identified in SCISA was not prohibited prior to this Act. The Act provides legal clarity to break down silos, foster information sharing and hopefully to lead to more effective operations in the national security space.

There is no oversight body that looks at the overall sharing between the 100 departments and organisations permitted to share information. As seen in Chapter 2 (2.1.4), users identified this as a potential concern.

---

105 Ibid, 28.
106 Ibid, 29.
Summary and Implications

As noted in Chapter 2 the accountability and oversight measures were considered inadequate for a majority of research participants, especially concerning intelligence oversight and oversight under SCISA.

Accountability and oversight mechanisms are built in through the audit power as executed under the Treasury Board Secretariat (TBS). The TBS may require internal audits and make non-binding recommendations.

The courts provide oversight over data processes, particularly when warrants are appropriate, though as seen in the decisions of Jarvis, Spencer, Wakeling, Telus and Rogers there is more court oversight for law enforcement than intelligence. These decisions have set boundaries to data access, use and disclosure. In theory the courts also play an oversight role over the intelligence agency CSIS in ensuring that they not unduly impede or restrict the rights and freedoms of Canadians as guaranteed in the Charter, but in practice, the jurisdiction appears ambiguous with instances of CSIS deliberately withholding information from both the oversight body SIRC, as well as in the case of X(Re) when questioned around data practices of requesting information from CSE.

The SIRC is comprised of members of the Privacy Council. They meet several times per year and act as an oversight body to CSIS. CSIS does not have an internal oversight entity for regular, consistent and daily oversight of its activities. SIRC is reliant on CSIS to supply them with the appropriate data and documents in order for them to properly exercise their oversight functions. They are not purview to the daily practices of CSIS with an internal perspective on how the agency functions in reality compared to how it functions on paper.

The CSE has a Commissioner that oversees its operations. The Minister of National Defence is the ultimate oversight entity through the issuance of Ministerial orders. When the Minister became away that bulk meta-data sets were not being sufficiently de-identified when given to the United States, he temporarily halted data flow until the issue could be fixed.

Under SCISA government agencies will be encouraged to share information with one another. While the RCMP, CSE and CSIS have oversight bodies, the other agencies listed in the act do not. Furthermore there is no ‘super’ oversight agency to take oversee the wider context of how information will be exchanged between all of these agencies.

### 3.7 Are principles and rules regularly reviewed?

The lens framework would require the regular, transparent review of principles and rules to ensure that the system delivers intended results efficiently and reliably, proportional to impacts on civil liberties, other legal rights and individual and commercial interests.

As examined in 3.6 the oversight bodies for CSIS, CSE and the RCMP submit annual reports to Parliament examining the various investigations, information controls and other items. Depending on the oversight committee, this is performed at regular intervals.

Big Data practices should be executed and reported in adherence to the principles found in Treasury Board documents including the above on information technology but again, these principles, guidelines and directives are not binding. This could prove a difficult task to perform well and in a meaningful way given the complexities of Big Data and its underlying technologies.
There are requirements for regular transparent review of the responsiveness of security controls for Federal agencies, and privacy controls for private organisations. The Office of the Privacy Commissioner may audit a private organisation’s practices. The Treasury Board may order an audit of an organization’s practices if they are a Federal government agency. They cannot, however, order an audit for intelligence agencies or the RCMP. These audits are performed by the oversight committees as stated in 3.6.

**Summary and Implications**

| Annual reports are tabled to Parliament around data practices of law enforcement and intelligence agencies. Where issues arise in the reports, the appropriate oversight entities have issued swift reviews. This has been seen with the Minister of Defence temporarily shutting down meta-data sharing with the United States, and the Office of the Privacy Commissioner announcing an investigation into the reporting habits of CSIS around data breaches. |

### 3.8 Is there a sufficient measure of transparency?

To the extent consistent with the need for operational secrecy, the framework would ensure that the nature of data accessed, analytic processes employed, and who has access are as transparent as feasible for those potentially affected by decisions, and those with an interest in policy- and rule-making.

The Treasury Board Policy on Information Technology Management addresses transparency and the important of regular review, and its relation to decision-making. The Transparency Section of the document addresses Principles including access, privacy, security, stewardess, whole-of-government approach and transparency. For transparency the principle is clear:

> Employees document actions and decisions in support of government programs and activities, and maintain information so that it is accessible to anyone who is authorized to have access, including those individuals exercising their rights to access information under the Access to Information Act and the Privacy Act. Managing information to support transparency and accountability also means reporting on performance in ways that are clear to Canadians and Parliament.

Transparency is not often directly referred to in the various relevant legislative instruments, or in the case law regarding law enforcement and intelligence use of data. As examined in section 3.2, interception warrants must be made known to the target after 90 days unless there are mitigating circumstances allowing for a court to make the interception a secret for up to 3 years. Annual reports by oversight committees refer to the number of times warrants were issues, requests were sought and the like.

#### 3.8.1 Individuals’ access to information collected about them

Individuals may make a request to ascertain whether information is being collected, used, disclosed and retained under PIPEDA (for private organisations), the Privacy Act (Federal government organisations) and Access to Information Act (Federal government organisations).

**PIPEDA**

Canadians may access personal information collected about them from any organisation subject to PIPEDA.
Privacy Act

Canadian citizens and permanent residents have a right of access provided by s 12(1) of the Privacy Act where an individual may request access to personal information contained about the individual in information banks and personal information under the control of a government institution. For the latter, the individual needs to provide enough specific information of the location of the information so that it may be reasonably retrieved (s 12(1)(b)).

3.8.2 Access to Information Act

The Access to Information Act\(^{108}\) allows an individual or organisation to file a request to access to information that a Federal agency may hold or have control of excluding classified document. Under s 2(1) the purpose of the Act is ‘that government information should be available to the public, but with necessary exceptions to the right of access that should be limited and specific, and that decisions on the disclosure of government information should be reviewed independently of government.’ The Information Commissioner may make recommendations as to the release of information.\(^{109}\)

3.8.3 Open government

The principle of open, accountable and transparent governance is referred to in legislation and policies most noticeable in the Directive on Open Government. As stated in s 3.1:

The Government of Canada’s commitment to open government is founded on the strong history of transparency and accountability first established with the enactment of the Access to Information Act in 1983 followed by the Federal Accountability Act in 2006 which introduced proactive disclosure. In 2012 the Government joined the Open Government Partnership and in June 2013 the Government endorsed the G8 Charter on Open Data.

The Directives is aimed at enabling ‘the proactive and ongoing release of government information.’\(^{110}\) The expectations of the Directive are stated in s 5.1. Paraphrased, these are:

- Use of information and data to support accountability
- To facilitate value-added analysis
- To drive socio-economic benefits
- To support meaningful engagement with government

Section 5.1 is aimed at ‘Canadians’ without reference as to whether opening datasets is geared towards Canadian individuals and private Canadian organisations to make use and reuse of government data, or if the expectation expands to include other agencies also making use of these open datasets. This has implications for Big Data use by government agencies.

---

\(^{108}\) Access to Information Act (R.S.C., 1985, c. A-1)
\(^{109}\) Ibid, s 36–37.
\(^{110}\) Directive on Open Government (Treasury Board), s 3.3.
Summary and Implications

Transparency in this context refers to data practices of agencies being shared with oversight bodies with recommendations for changes following. Transparency has often meant how many times and with who has information been exchanged. It has less often meant transparency in how the underlying technologies function. This may be explained by secrecy around capability (with good reason), and that there isn’t a history of technical transparency or what is now being called algorithmic transparency.

There will need to be more robust and comprehensive reviews not only of data practices and the underlying algorithms of Big Data systems to address the objectives. This will better to help to ensure that the objectives are being met, are valid, and are reasonable and proportionate with their intended purpose.
4. CONCLUSION

This study of Canada was undertaken as a part of a broader comparative study of Big Data and national security (Big Data Technology and National Security: Comparative International Perspectives on Strategy, Policy and Law in Australia, the United Kingdom, the United States, New Zealand and Canada). An overview of the research project, including the research questions, methods and sources of empirical data, and indicators of a legal and policy framework that supports ‘desirable and effective’ Big Data practices can be found in the Methodology Report. Three separate Country Reports – on Australia, UK, and Canada (the current Report) – provide details of the empirical findings and legal analysis in each jurisdiction. Comparative perspectives and recommendations for law reform in Australia are set out in the Executive Summary and Recommendations.

This chapter summarises the key findings and insights from the Canada study.

Interviews were conducted from 15 October 2015 to 26 February 2016 and the legal analysis presents the law as it stood on 1 June 2016.

4.1 Using Big Data for national security: Stakeholders’ perspectives

The empirical research in Canada was designed to provide a comparative dimension to inform our analysis of law and policy for the use of Big Data for national security in Australia. The Canada research is based on face-to-face interviews (one interview was conducted over the telephone) with 11 research participants who were working or had worked in operational agencies (six participants), policy (one participant), independent organisations (two participants) or non-government bodies (two participants). All were selected because they were able to provide relevant information on the use of data or regulation of data use for law enforcement or security intelligence. Time and resource constraints necessitated a relatively modest sample size. These interview findings are therefore presented with references to the Australian results. As noted in Chapter 2, the Canadian and Australian samples were drawn from broadly similar types of organisations (although technical organisations were excluded in Canada) but there were some notable differences in the research participants. The two samples may therefore not be directly comparable.

The interviews explored the following broader themes:

- Current use of data
- Current concerns regarding access to data
- How problems can be overcome
- Big Data: potentials, limits and risks
- Regulation
- Values and Big Data

The goal of this report is to capture understandings, perceptions and views of individual research participants on a range of issues. It is important to emphasise that the empirical findings presented in this report provide a snapshot of the views and perceptions of research participants only. These views and perceptions may or may not be based on a comprehensive or accurate understanding of the issues involved. Given that the sample size is relatively small and not necessarily representative of the population of stakeholders in Canada, the findings are meant to indicate issues and not to be read as a comprehensive coverage of all relevant information. We do not attempt here to evaluate or correct research participants’ views, although we have included cross-references to other sections in the report where appropriate.
4.1.1 Current use of data

The three Canadian research participants from operational organisations emphasised the importance of using data not only to identify trends but to enable better business management. As in the Australian study, there were also diverse responses including predicting trends, disruption, intelligence for investigations, business intelligence and efficiency metrics.

There is sharing of data between agencies domestically and internationally with different rules applying to different contexts. Users identified that the default rule in Canada is that sharing between domestic agencies is allowed unless expressly prohibited. In the international context it was more complicated. Users pointed out that there had been problems with sharing in the past leading to Charter of Human Rights violations including torture. Data sharing among agencies and with foreign counterparts involves decisions that are not easily automated. This led to the so-called O’Connor Recommendations discussed in Chapter 1.

Sharing information occurred between government organisations (law enforcement, other related to national security), non-government organisations, and between foreign agencies. The extent of sharing was not identified in the interviews. The participants also identified three aspects that did not arise in the Australian context. These were: over-classification of data preventing sharing; there are few regulatory impediments to sharing information between Canadian agencies; and that there were concerns raised with regards to sharing information with foreign agencies.

4.1.2 Current concerns regarding access to data

As in Australia, legal requirements were the primary concern among research participants from operational organisations. While privacy controls were mentioned by participants from both countries, technical issues, and ownership and trust issues were also important factors in the Canadian responses. Issues around sharing data and lack of capacity to process data were seen as important and unresolved issues from the Canadian responses including how trust has previously been done person to person, and how there were growing concerns around the lack of sharing controls with foreign agencies.

Three main concerns were raised, however, legal requirements made up the majority of concerns among research participants. While privacy controls were mentioned from research participants from both Canada and Australia, sharing controls and ownership/trust issues were important factors in the Canadian responses. Technical issues were also present in Canada.

Legal requirements: The most frequently cited concern related to real or perceived legal requirements, including in relation to sharing and privacy issues. Participants readily referred to the information sharing aspects of the new piece of legislation known as Bill C-51.

Technical issues related mainly to matters such as data format, data ‘silos’, non-availability of historical data, the agency’s ability to deal with the volume of data, and the continued use of legacy technology.

Data ownership and trust between agencies or individuals were the two factors that appear to explain some of the reluctance to share data. Reference was made to cultural issues (reluctance to trust quality of data from another agency; legal responsibility for use of data; and general control issues) that make data sharing challenging.
4.1.3 How problems can be overcome

While only two research participants directly answered the question how can problems be overcome, there were points in the interviews when discussing other concerns and risks where resolving problems was identified. The two participants both identified cultural change as important in addressing concerns including change in sharing, ownership and trust, as well as resolving technical concerns. Other inferences drawn generally from the other interviews included resolutions to concerns through providing sufficient resources both for the staff and for acquisition of technologies.

4.1.4 Big Data: potentials, limits and risks

What is Big Data?

‘Big Data’ is a term without a single precise meaning; rather it is used to articulate a range of practices. In the context of national security and law enforcement, research participants’ definitions of Big Data were focussed on both technical and user requirements. The main requirements relate to handling volume, analytic capacity to provide useful and reliable information, and dataset integration.

Capability of Big Data

In terms of capability, Big Data was seen by research participants as involving analytic capacity, ‘rich’ data, the ability to identify patterns and trends, improved efficiency and effectiveness, and enabling data-driven decision making. Not every participant saw an advantage to Big Data, and three cautioned against unrealistic expectations while two believed that governments would be very slow to uptake Big Data, and even slower to do so in a cost effective way. They thought that a lack of culture and training could make Big Data less relevant as decision-makers were more likely to be traditional in social science backgrounds without fully understanding how big data methodology differs.

Use of Big Data and Data Analytics

Only three participants in operational organisations stated that they were using Big Data, while the other participants stated that they were just starting to use Big Data visualisation tools, but the uptake had so far been slow. This may suggest that their conceptions of Big Data and its capability and value were not necessarily based on first-hand knowledge or experience with this technology, however, two of these participants worked with Big Data on a daily basis and one programmed bespoke tools used within their organisation.

Most participants from operational organisations indicated that they have been using data analytics and statistical analysis for quite some time, but the use of machine learning or predictive tools was not mentioned. As in Australia organisations were using both off the shelf and custom tools.

Barriers/challenged to using Big Data

Barriers to the use of Big Data on the whole were similar in Canada to those in Australia. Legal requirements were presented as a challenge to Big Data. Ironically it was a lack of adequate privacy laws that was perceived as the barrier; not that privacy laws prevented Big Data usage. Some research participants discussed how the Privacy Act was out of date and unsuited to technologies in general generating a hesitancy and reluctance to move toward more invasive technologies, and that the Act contained much weaker provisions than PIPEDA which governs private organisations.
Research participants identified cultural and technical barriers as a significant challenge. There were a variety of cultural barriers to greater use of Big Data for law enforcement and national security. These include the fact that Big Data is unlikely to be used unless there is institutional support and appropriate levels of trust, and confidence in technology among users.

**Risks of using Big Data**

Invasion of privacy was a risk most frequently nominated by the participants in Canada, and Australia. There were two new risks identified by Canadians: danger of confusing correlation with causation, and litigation. Three out of eleven participants believed that insufficient training / danger of confusing correlation with causation was a risk that could result in harms including privacy, economic and discrimination. One Canadian and one Australian participant also thought that not using Big Data could be a risk.

Overall, the main identified risks related to privacy, data integrity and ownership, and general technical issues. Both operational and policy groups expressed the view that there were risks to privacy. A participant who both worked with Big Data on a daily basis and who developed Big Data tools highlighted that privacy was less of an issue when compared to discrimination. Other participants used the term ‘harm’ to include privacy risks.

**Who is exposed to these risks?**

‘Everyone’ was the most popular response to who is exposed to risk by research participants in both Canada and Australia. While four participants in the Australian sample identified minorities and marginal people as being exposed to risks, only one participant in Canada mentioned this.

**Management of Big Data Risks**

Research participants discussed a range of potential ways to mitigate against risks. These included access controls more in line with the restraints imposed on the private sector. There was a further suggestion to tighten restrictions on third party data sales. More data security requirements were also suggested as was better education of the public about the actual versus perceived risks of Big Data.

**4.1.5 Regulation**

**Laws, regulations, and internal guidelines**

Two regulatory frameworks were identified by the majority of research participants. These were Privacy (Privacy Act and privacy frameworks in general) and Sharing (C-51 / SCISA). Approximately half of the participants also identified the Charter, and Treasury Board Policies and Directives (these formed the main types of general guidelines for issues) and agency specific legislation.

Participants from different roles and sectors equally recognised Privacy legislation, sharing legislation of C-51/SCISA and the Charter.

**Accountability, transparency and oversight mechanisms**

No research participants stated that there was not a need for agencies to share information, especially for national security purposes. All participants save for one believed that there was not sufficient transparency and oversight. Concerns were raised over whether increased transparency would be meaningful absent increased education and training to understand
Big Data systems. Algorithmic transparency was regarded as a desirable outcome only if would be sufficiently understood by decision makers.

Information silos were identified at different points in the interviews as concerns. However Canadian participants also identified the problem of oversight silos and the need for better oversight appropriate for the new formation of sharing under SCISA with appropriate resources to ensure that oversight is robust.

The lack of accountability mechanisms was not directly mentioned in the interviews though it is difficult to separate comments about oversight with those of accountability. Accountability issues arose more in the context of culture of data ownership responsibility creating a reluctance to share data. This was discussed as a barrier to governments sharing data, as well as a potential barrier to Big Data uptake.

*Appropriateness and effectiveness*

There is no clear division in Canada between sectors. Unlike the case in Australia, there is not a clear division between those in the research/NGO sectors who were sometimes critical (particularly about oversight) and those in the government sector who were generally uncritical, or focussed on restrictiveness. In Australia there were 22 on the positive side with only 3 on the negative side. In Canada this distribution was more equal with 4 positive, and 5 negative. Research participants from all sectors and roles expressed strong concerns with appropriate oversight mechanisms.

*Perceived shortcoming in law and regulation and proposals for reform*

Research participants raised general proposals for reform noting that laws around privacy and oversight required updating. There was an additional call for updated Guidelines and Directives for sharing data with foreign agencies in an easier to understand and transparent fashion that could be harmonised across agencies.

Similar to the Australian study, participants called for reduction of the complexity and to enhance harmonisation of practices across agencies. Where research participants from the Australia Study expressed the possibility of reducing ‘red tape’ without reducing oversight, Canadians did not address ‘red tape’ issues. Their concerns were about increasing the oversight framework which is viewed by the majority of participants as inadequate. This may be due to the regulatory framework explored in Chapter 3 where Canada has less restrictions around sharing information when compared to Australia.

*Regulation by design*

Data integrity and cost were the only three design features that were taken into account by each of the three research participants, all having worked in operational organisations. This suggests that data practices are not unified across departments. The question about privacy by design yielded an interesting result where one organisation placed this responsibility with the data owner, another said that they didn’t factor privacy, while the last research participant laid out extensive measures used to assess and minimise privacy concerns.

4.1.6 Values and Big Data

*Protections where individuals consents to use of sharing of their data (see Methodology Report 5.2.5)*

As in Australia, research participants mentioned issues around the ‘quality’ of consent, continuing limits on its use (including proper purpose). The issue of expiry or revocation was raised by both the Australian and Canadian research participants. Two Canadian participants
expressed concerns over implied and opt-out standards calling for opt-in and express consent.

**Attitudes to privacy**

As in the case of Australia, there were varied views on the importance of privacy, particularly in the context of serious imminent threats. No-one expressed the view that privacy concerns should not be paramount in a situation of serious imminent threat provided that it could be justified.

**Privacy versus Security: A scenario (see Methodology Report 5.2.2)**

Three of the Canadian research participants gave the same answers to the scenario whether the context was kidnapping, child sexual assault or terrorism. They indicated that there are sufficient legal provisions and flexibility to allow law enforcement to move to more intrusive measures in order to curtail the threat. Only two participants indicated potential problems such as abuse or scope creep, and only one participant was uncomfortable with the use of Big Data techniques including the escalation of context but these were recorded as using tools with caveats.

**What transparency is required (see Methodology Report 5.2.8)**

Transparency is a challenge for national security and law enforcement agencies. Transparency can ensure that errors and biases are addressed, is a deterrent to misuse of data, is an important public value, and is an important element of democratic accountability. However, operational secrecy is also crucial for effectiveness in many situations.

Unlike in Australia, the four Canadian research participants who responded were not concerned about competing priorities in increasing transparency. In the Australian study there were differences between transparency of the data and of the analysis outputs. In Canada there was no differentiation. The Canadian responses instead focussed more on utility, education, limits and the importance of trust and rules when sharing information between agencies.

**How views align with others**

The views reflected in the Canadian sample were different from those in the Australian sample. In Australia, research participants formed four clusters (rights-based NGOs and community groups, victim-aligned NGOs, industry groups, and government agencies) whereas in Canada rights-based NGOs and community groups, or victim-aligned NGOs were not interviewed. In Australia, differences could be explained in part by the fact that different sectors had different levels of knowledge about how data is actually used and how this use is regulated. In Canada, however, this distinction wasn’t as apparent. This could be due to the fact that three out of the five policy research participants had previous roles in intelligence and law enforcement such that their views would have been formed from having seen the issues develop from different perspectives.

**Resolving conflicts in values**

Canadian research participants did not provide responses to this line of inquiry.

**Source of views**

Four out of five research participants reported three main sources of their views: professional or personal knowledge, evidence or academic papers/reports, and media/blogs, two nominated ‘broad consultation’, and two ‘contact with experts’. Compared with the
Australian sample, the Canadian research participants appeared to rely more on sources of information external to their professional or personal experience.

4.2 Big Data, law enforcement and national security: The legal environment in Canada

Early in the study, it became clear that Canada like Australia has neither adopted Big Data-specific strategies, policies, laws, regulatory frameworks, practices and technologies relating to law enforcement and national security, nor were there appropriate, comprehensive frameworks for private organisations use of Big Data. There are, however, a host of measures that are directly or indirectly relevant to Big Data applications. The Information Sharing Act for example encourages sharing, inclusive of bulk data sets, between different agencies involved in national threats.

The initial set of indicators developed in the Methodology Report, though not necessarily complete, represents a useful starting point for an appropriate overarching legal and policy framework. Collectively, the presence of these indicators would indicate a framework that can support the effective use of advanced analytics and large data sets for law enforcement and national security purposes, while respecting the rights and interests of all stakeholders (including data subjects, the broader community and the economy), addresses proportionality and evidence-based justification, and ensures comprehensive identification and management of risk and opportunities.

The indicators, discussed in greater detail Chapter 5 of the Methodology Report, are clustered around the following questions:

1. Is access for data mining enabled?
2. Are legal controls comprehensive and proportionate?
3. Are legal rules clear, principle-based, consistent and instructive?
4. Is integrity of data and systems supported?
5. Are data and systems protected?
6. Is accountability maintained?
7. Are principles and rules regularly reviewed?
8. Is there a sufficient measure of transparency?

4.2.1 Is access for data mining enabled?

Canada does not distinguish between government-held data, open source data, privately-held data and data held by foreign governments. Canada distinguishes instead by the type of organisation holding the data: government, private, or foreign government.

Federal government agencies access and control measures are derived from three main sources: the Privacy Act, SCISA and Treasury Board Guidelines and Directives. Law enforcement and intelligence agencies (RCMP, CSIS and CSE) are bound by the Privacy Act and SCISA, while the Treasury Board Guidelines and Directives are only meant to provide guidance in various areas around information technology, privacy, and data systems and practices. Treasury Board Guidelines and Directives are not legally binding instruments.

The Privacy Act imposes some (albeit few) requirements on agency collection and disclosure of data but is not as comprehensive as the Australian Privacy Principles or (as will be explored below) the federal private sector privacy principles in PIPEDA. The purpose of the Privacy Act is to provide an avenue for an individual to ascertain what and how the government collects information about them. The focus is not on providing a comprehensive set of principles for privacy practice amongst Federal government agencies. The Privacy Act
of 1983 has not been amended since it entered into force. It is silent on data mining, data analytics, de-identification and, as was seen in the interviews in Chapter 2, is viewed as outdated in the context of protecting privacy in an era of technical advancements. There are no prohibitions on disclosure of data (personal information) to a third party for research or statistics if it is required for the purpose. The assumption is that where personal information is de-identified is may be disclosed and used by other agencies.

SCISA does not establish limits and rules around the collection, use and disclosure of information between government agencies (those listed in the legislation including law enforcement, intelligence agencies and other agencies connected to ‘national threat’). The purpose of the Act is to encourage and facilitate sharing amongst designated agencies. It also does not mandate that agencies share information with one another.

The Treasury Board guidelines and directives provide some guidance on data practices but these are not binding on government agencies. The Web Analytics guidelines suggests de-identification of personal information, and provides guidance on disclosure of data to third parties. Disclosure should be pre-authorised, and data should be destroyed 18 months after it is received. As seen in Canada (Information Commissioner) v. Canada (Commissioner of The Royal Canadian Mounted Police), courts view Treasury Board documents are persuasive only when interpreting information obligations.

Warrants are required for federal agencies to intercept private communications as specified in the Canadian criminal code. The courts in Jarvis, Wakeling, Spencer, Telus and Roger provide additional elements of appropriate warrants around data access, use.

The legislation and regulatory framework does not refer to data held by foreign governments. Only data about Canadians or those located in Canada was dealt with in the regulatory framework which required data about Canadians be de-identified when given to foreign governments. In addition to this, the O’Connor Recommendations required caveats be placed when identifiable data was given to foreign governments such as stating which institutions are entitled to access the information, as well as procedures should any changes be permitted to how and whom the information is shared with.

Federal private organisations are governed by PIPEDA. The privacy principles identified in PIPEDA are similar to the Australian Privacy Principles. These include, for example, informed consent, security principles, and destruction and retention principles. Crown corporations such as Canada Post are bound by the provisions of PIPEDA. Memoranda of understandings are written for sharing information between federal private organisations. Ministerial Authorisations govern metadata practices including sharing between federal private organisations and government agencies.

The Canadian position on controls of data, and in particular controls around privacy, is significantly more complex than the principle based approach in Australia. Federal government agencies must adhere to the Privacy Act 1983. The Act has not been amended since 1983 and is ill-equipped to deal with many issues that arise in the context of technology. This must be contrasted to PIPEDA which governs private organisations, is principle based and has been amended on numerous occasions in order to accommodate privacy concerns generated by the use of new technologies.

Intelligence agencies such as CSIS and CSE follow Ministerial Guidelines on privacy and information disclosure. Warrants are required by CSIS to obtain information about a

---

111 Canada (Information Commissioner) v. Canada (Commissioner of the Royal Canadian Mounted Police) [2003] 1 SCR 66.
Canadian or person in Canada. The situation outside of Canada is less clear as is the requirements of data exchange between foreign agencies.

In theory any bulk datasets flowing across border such as meta-data must be de-identified. There are no rules on re-identification once the data crosses borders. When information is exchanged across borders it is often now done with caveats (post O’Connor Recommendations) but such caveats discuss limits on third party disclosures and not re-identification or what type of analytics is allowed to be run on data sets. Re-identification in Canada is not clear cut but the Supreme Courts’ decisions in Wakeling, Jarvis and Spencer indicate that where there is an expectation of privacy any use of data for an investigation leading to criminal chargers will require a warrant. It is likely that a warrant will be required down the road for re-identification performed by agencies within Canada.

4.2.2 Are legal controls comprehensive and proportionate?
See 3.1.

4.2.3 Are legal rules clear, principle-based, consistent and instructive?
The Canadian framework strives for clarity and transparency yet examination of the various polices, directives and legislation does not provide a clear picture for many data practices.

The Treasury Board documents are non-binding. The Privacy Act provisions are out-of-date and are not principle based. A focus on privacy principles and standards in data practices is required to ensure consistency while maintaining flexibility across contexts. While the Treasury Board documents are both flexible and principle based they are merely persuasive. In an area that directly impacts on rights and freedoms guaranteed under the Charter binding legislative provisions seem more appropriate than mere guidelines. Additionally, there are no Treasury Board guidelines and directives looking at more advanced data analytics (reference to Web analytics such as cookies).

4.2.4 Is integrity of data and systems supported?
Data integrity is regulated in the federal private sector in Canada but not in the public sector. Relevant documents addressing data integrity issues are non-binding Treasury Board documents related to information technology. There is no general data integrity principle in either the Privacy Act or in the privacy related guidelines from the Treasury Board. The exception is privacy in employment context where data integrity is required; this is likely because employment is the only area where Treasury Board Guidelines and Directives are binding legal instruments (as discussed in 3.1 and 3.2).

Big Data tools and culture are well known for their capacity to accept data which is less reliable, complete, accurate, up to date or relevant than usually required for data systems. But while the tools may deliver output from low integrity input or unverifiable assumptions, and preserving provenance may allow for humans to give less weight to poor quality data, the integrity of the outcome remains uncertain until the Big Data system is fully implemented and regularly tested.

Law enforcement processes producing criminal evidence is guided by the rigour that accompanies testing in an adversarial, open court process with strict rules of admissibility, relevance and probative value.\(^{112}\) Criminal and national intelligence processes, on the other hand, necessarily rely on less rigorously tested and verified information. As is appropriate to

\(^{112}\) There are extensive provisions about information use in Evidence Acts, Rules of Court, case law and other laws.
the nature of their task, accepted standards of ‘proof’ or probative value are typically below the standard of ‘beyond reasonable doubt’. In addition, these processes are often necessarily secret and citizens who may suffer negative consequences as a result of incorrect data do not have the opportunity to challenge or correct the data. While this is a necessary feature of the terrain, and of necessity less reliable information has to be utilised, the use of Big Data models for decisions which have impacts on individuals without the rigorous testing of a court process raise questions about how to set the appropriate standards and expectations of integrity, probative value and relevance.

Intelligence analysts are skilled to deal with data that has differing levels of integrity. Action may be taken on lower quality data where a significant national security breach may be pending. Where, however, there is a less compelling or serious harm involved, making decisions affecting individuals on lower quality information may be disproportionately adverse. Legal rules do not currently regulate such intelligence decisions but clearer rules may be required for Big Data systems to ensure that uncertainty is preserved so the inferences/predictions can be given estimates of truth in line with the provenance of the underlying data. This may be consistent with the current rules (which are beyond the scope of the report).

Big Data tools, more than other intelligence methods, may be used in situations far removed from the source of the information on which they depend, the knowledge of those with actual experience of the source, and the consequences of decisions which they may suggest. One important aspect of integrity is to ensure that appropriate efforts are made to consider the logical and inferential reliability of the output as a basis for making decisions about individuals.

As noted in the literature review in chapter 2 of the Methodology Report, Big Data analytics, especially prediction of intrinsically uncertain future events, are typically based on statistical or algorithmic correlation, but legal consequences and the notion of responsibility is more often tied to causation. This potential divergence between analytical methods and a requirement of being able to attribute causal responsibility may restrain inappropriate interpretation of correlation. This is in particular so in cases where a decision could only be justified on the ground that causality is demonstrated (either because an individual is affected, or because it is assumed that a policy change will have a particular impact). No comprehensive provisions in statutory or other rules or controls specifically address this problem.

4.2.5 Are data and systems protected?

Security safeguard mechanisms are for federal government agencies are similar to privacy mechanisms. There is little by way of binding legislative provisions to ensure that data is secure. There are many different Treasury Board documents such as data breach notification ‘Directive on Privacy Practices’ and ‘Government Security Policy’ but these are not binding. This discretion on whether to report data breaches is seen in the empirics where CSIS only allegedly had one breach which was reported. The RCMP reported half of their breaches. While the CSE had breaches they did not elect to report any. This potential under-reporting has led the Privacy Commissioner, Daniel Therrien, to launch an investigation into CSIS’s breach reporting.

113 This is an area where discussion of scope creep is relevant: acceptance of the need to use lower quality data in ‘extreme’ cases may lead to such use in less ‘extreme’ cases.
This is to be contrasted with the federal private sector’s obligations to keep data secure under PIPEDA. PIPEDA also includes data breach notification law with the Office of the Privacy Commissioner where fines of up to $100,000 may be imposed for non-compliance.

4.2.6 Is accountability maintained?

As noted in Chapter 2 the accountability and oversight measures were considered inadequate for a majority of research participants, especially concerning intelligence oversight and oversight under SCISA.

Accountability and oversight mechanisms are built in through the audit power as executed under the Treasury Board Secretariat (TBS). The TBS may require internal audits and make non-binding recommendations.

The courts provide oversight over data processes, particularly when warrants are appropriate, though as seen in the decisions of Jarvis, Spencer, Wakeling, Telus and Rogers there is more court oversight for law enforcement than intelligence. These decisions have set boundaries to data access, use and disclosure – in theory the courts also play an oversight role over the intelligence agency CSIS in ensuring that they not unduly impede or restrict the rights and freedoms of Canadians as guaranteed in the Charter, but in practice, the jurisdiction appears ambiguous with instances of CSIS deliberately withholding information from both the oversight body SIRC, as well as in the case of Re(X) when questioned around data practices of requesting information from CSE.

The SIRC is comprised of members of the Privacy Council. They meet several times per year and act as an oversight body to CSIS. CSIS does not have an internal oversight entity for regular, consistent and daily oversight of its activities. SIRC is reliant on CSIS to supply them with the appropriate data and documents in order for them to properly exercise their oversight functions. They are not purview to the daily practices of CSIS with an internal perspective on how the agency functions in reality compared to how it functions on paper.

The CSE has a Commissioner that oversees its operations. The Minister of National Defence is the ultimate oversight entity through the issuance of Ministerial orders. When the Minister became away that bulk meta-data sets were not being sufficiently de-identified when given to the United States, he temporarily halted data flow until the issue could be fixed.

Under SCISA government agencies will be encouraged to share information with one another. While the RCMP, CSE and CSIS have oversight bodies, the other agencies listed in the act do not. Furthermore there is no ‘super’ oversight agency to take oversee the wider context of how information will be exchanged between all of these agencies.

4.2.7 Are principles and rules regularly reviewed?

Annual reports are tabled to Parliament around data practices of law enforcement and intelligence agencies. Where issues arise in the reports, the appropriate oversight entities have issued swift reviews. This has been seen with the Minister of Defence temporarily shutting down meta-data sharing with the United States, and the Office of the Privacy Commissioner announcing an investigation into the reporting habits of CSIS around data breaches.

4.2.8 Is there a sufficient measure of transparency?

Transparency in this context refers to data practices of agencies being shared with oversight bodies with recommendations for changes following. Transparency has often meant how many times and with whom has information been exchanged. It has less often meant
transparency in how the underlying technologies function. This may be explained by secrecy around capability (with good reason), and that there isn’t a history of technical transparency or what is now being called algorithmic transparency.

There will need to be more robust and comprehensive reviews not only of data practices and the underlying algorithms of Big Data systems to address the objectives. This will better to help to ensure that the objectives are being met, are valid, and are reasonable and proportionate with their intended purpose.
APPENDIX

Big Data Technology and National Security

A. Interviews with law enforcement and intelligence officials – Canada

Introductory Information

Thank you for agreeing to an interview. Before we start I would like to tell you a bit more about the study and what we hope to achieve from the interviews. As you would be aware from the Participant Information Statement, the main aim of this project is to examine the policies, regulatory approaches, processes and strategies used by Australia and selected partner countries to balance the management and exploitation of Big Data for law enforcement and national security purposes, while safeguarding confidentiality and security of sensitive personal information, as well as the accuracy of data sets. This research project is not concerned with information that may be private, classified, or in relation to specific criminal offences. You are requested not to disclose such information during the interview. We would like to also remind you that anything we talk about will remain confidential to the project and if we use anything you say in this interview in our publications, we will make sure that you will not be identifiable.

Current Position

1. Please describe the responsibilities of your current position and the organisation and team or unit in which you are employed.

   [NB: if you have any concerns about being identified, we will not include specifics about your position/responsibilities that could be used to identify you.]

2. Could you tell us

   (a) what your education and training background is,

   (b) how long you have been in this position, and

   (c) about your work experience prior to the current position?

General

3. When does digital/computer technology hinder you in your work and when is it particularly helpful?

Data Sources, Access and Sharing

I am going to ask some questions around data sources, access and sharing. In these questions, I use the term “data” broadly to capture records, information and intelligence.

4. What types of data do you (or your unit) use in your work?

5. Does your unit share data with other agencies, and if so, which ones?

6. What kind of data is shared – is it raw or summarised; identified or de-identified?

7. What are you major concerns in relation to data access from other agencies or sharing data with other agencies?

8. Do these problems affect your (or your staff’s) morale or sense of professionalism?

9. How can these problems be overcome?
Data Analytics

10. What do you (or your unit) mainly use these data for?
   (Probe: law enforcement, investigation, crime prevention, security intelligence, meaning of “national security” if used).

11. What do you (or your unit) do with this data in order to pursue [law enforcement investigation/crime prevention/security intelligence etc as described above] purposes?
   (probe e.g. statistical reports, mapping, linking with other data, manual filing or note-taking, following investigative leads)

12. (a) Do you (or your unit) do data visualisation or data analysis?
   (b) If so, what techniques or software do you (or your unit) use?
   (c) Are these off-the-shelf or custom tools? (Probe eg geospatial mapping)

13. What are the most serious issues/problems that may prevent you (or your unit) making greater use of data analytics?
   (Probe: data mining, regression as examples; issues such as expertise, training, data quality, access to data, etc)

14. Do you think your agencies’ access to data and analytical tools is better or worse than
   (a) other agencies,
   (b) your foreign counterparts and
   (c) the private sector?
   (If the answer is worse, probe impact, the level of concern and any actions that may be suggested)

Big Data

15. This research project is concerned with the use of Big Data. The term ‘Big Data’ has been used by people in a number of ways. How would you define Big Data?

16. As far as you know, what is Big Data capable of doing that “ordinary data” can’t?

17. To what extent are you (or your unit) making use of Big Data tools in your work?
   (Probe: would they describe the techniques in answer to earlier questions as “Big Data”?)

18. What are the most serious issues/problems that may prevent you (or your unit) from making more use of Big Data?
   (Probe: Are there issues with data formatting, particularly consistency across agencies? Are there issues with data quality / does data quality vary depending on the agency concerned?)

19. What do you see are the risks of using Big Data for law enforcement or security intelligence?
   (Probe – risks to other people, risks for quality of decisions, risks due to (wrong, poorly understood) assumptions inherent in algorithms) (Follow up if not obvious – Who is affected by these risks?)
Regulation

20. As you know, there are laws, regulations, guidelines and procedures governing the use of data by law enforcement or security agencies, including mechanisms for accountability and oversight.

   a. What laws, regulations, guidelines and procedures govern your use of data in your work? (Ask if we can obtain copies if possible, or find out where they are located)? Do any of these regulate Big Data techniques as such? Any other accountability or oversight mechanisms?

   b. In your view are these laws, regulations, procedures, guidelines (including accountability and oversight mechanisms) appropriate and effective? In particular, what do you think these are meant to achieve and do you feel they are successful?

   c. What are the shortcomings of the current laws, regulations, guidelines and procedures? How do you think they should be changed?

21. How do you think the law should strike a balance between privacy/individual rights and public concerns such as national security, terrorism and serious crimes?

   (If so, probe how this balance can be achieved).

   Thank you very much for taking the time to be interviewed. Your input is much appreciated.
Big Data Technology and National Security

B. Interviews with technologists/designers – Canada

Introductory Information

Thank you for agreeing to an interview. Before we start I would like to tell you a bit more about the study and what we hope to achieve from the interviews. As you would be aware from the Participant Information Statement, the main aim of this project is to examine the policies, regulatory approaches, processes and strategies used by Australia and selected partner countries to balance the management and exploitation of Big Data for law enforcement and national security purposes, while safeguarding confidentiality and security of sensitive personal information, as well as the accuracy of data sets. This research project is not concerned with information that may be private, classified, or in relation to specific criminal offences. You are requested not to disclose such information during the interview. We would like to also remind you that anything we talk about will remain confidential to the project and if we use anything you say in this interview in our publications, we will make sure that you will not be identifiable.

Current Position

1. Please describe the responsibilities of your current position and the organisation in which you are employed.
   [NB: if you have any concerns about being identified, we will not include specifics about your position/responsibilities that could be used to identify you.]

2. Could you tell us
   (a) what your education and training background is,
   (b) how long you have been in this position, and
   (c) about your work experience prior to the current position?

Big Data – Capabilities

3. This project is concerned with the use of Big Data. The term ‘Big Data’ has been used by people in a number of ways.
   (a) How would you define Big Data?
   (b) What does it mean in the context of your work?
   (c) How does it relate to other terms you might use? [probe data science, data analytics]

4. (a) Do you use Big Data in your work/systems?
   (b) What role do Big Data techniques have in your work/systems?
   (c) What is your role in relation to these?

   (Probe – if treat “Big Data” as a narrow concept ask In your organisation/system, what do you use data analysis for?)
5. (a) What types of data analysis do you or does your organisation do?
(b) What are the outputs?
(c) How reliable/accurate are these outputs?

6. (a) Who are the users of your product/system?
(b) Who can access data within the system?
(c) What mechanisms are used to ensure the security and privacy of data within the system?

7. In your organisation/system, what are the main challenges you face with respect to Big Data or data analysis?

8. What do you see are the opportunities or possibilities that [data analysis/data science if they used these terms] or Big Data can open up for law enforcement and security intelligence?

9. What data analytic and data visualization tools or software do you use when dealing with large data sets? What do these tools provide you with? Are they useful?

10. (a) What do you know about Big Data or data science/analytics that everyone in the field will know in five years?
(b) How would you improve the way your organisation designs systems or builds tools for working with national security and law enforcement data?

**Risks and regulation**

11. (a) What risks or issues do you think arise or will in the future arise in relation to the use of Big Data or data analytics, particularly in law enforcement and national security contexts?
(b) In particular, are there any risks associated with your work or product?
(c) Who is exposed to these risks?
(d) How should these risks be managed?

12. As you may know, there are laws, regulations, guidelines and procedures governing the use of data by law enforcement or security agencies, including mechanisms for accountability and oversight.
   a. What laws, regulations, guidelines and procedures affect how you design systems for the use and analysis of data within law enforcement and national security agencies?
   b. Do any of these regulate Big Data techniques as such?
   c. What advice would you give policy-makers on the use of Big Data or data analytics/data science for law enforcement or national security purposes?

13. (a) How important is it that outputs of your system are reliable and accurate?
(b) How tolerant of invalid, unreliable, corrupted or non-relevant data can your system afford to be?
### Design Issues

14. Who sets the design parameters for your product/system?

(Probe to whom are you or your organisation responsible in designing your product/system?)

15. To what extent can some of the risks of data analytics be mitigated through the design of analytical tools? For each of the following issues, please indicate whether you take it into account in your design (Yes/No), and if so, how:

<table>
<thead>
<tr>
<th>Issues</th>
<th>Yes/No</th>
<th>How is it taken into account?*</th>
</tr>
</thead>
<tbody>
<tr>
<td>Protection of privacy and personal information security</td>
<td></td>
<td>Probe – privacy by design / privacy engineering</td>
</tr>
<tr>
<td>The confidentiality of communications (data in transit)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Data integrity, [ie that information held is accurate, current, relevant and not misleading]</td>
<td></td>
<td>Probe – data cleaning/scrubbing; does system have built in signposts for risks of invalid, unreliable, corrupted or non-relevant data</td>
</tr>
<tr>
<td>Testing and evaluation</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Comprehensibility to decision-makers</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Avoiding discrimination</td>
<td></td>
<td>Probe eg racial, religion</td>
</tr>
<tr>
<td>Potential for any de-identified data to be re-identified</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Agency inter-operability</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Cost</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

*For how taken into account, can probe separately (1) data scrubbing, (2) ETL (Extract, Transform and Load), (3) database work (SQL).

Thank you very much for taking the time to be interviewed. Your input is much appreciated.
C. Interviews with policymakers, citizen groups – Canada

Introductory Information

Thank you for agreeing to an interview. Before we start I would like to tell you a bit more about the study and what we hope to achieve from the interviews. As you would be aware from the Participant Information Statement, the main aim of this project is to examine the policies, regulatory approaches, processes and strategies used by Australia and selected partner countries to balance the management and exploitation of Big Data for law enforcement and national security purposes, while safeguarding confidentiality and security of sensitive personal information, as well as the accuracy of data sets. This research project is not concerned with information that may be private, classified, or in relation to specific criminal offences. You are requested not to disclose such information during the interview. We would like to also remind you that anything we talk about will remain confidential to the project and if we use anything you say in this interview in our publications, we will make sure that you will not be identifiable.

Current Position

1. Please describe the responsibilities of your current position and the organisation in which you are employed.
   [NB: if you have any concerns about being identified, we will not include specifics about your position/responsibilities that could be used to identify you.]

2. Could you tell us
   (a) what your education and training background is,
   (b) how long you have been in this position, and
   (c) about your work experience prior to the current position?

Big Data – Capabilities

3. This project is concerned with the use of Big Data. The term ‘Big Data’ has been used by people in a number of ways. How would you define Big Data?

4. As far as you know, what is Big Data capable of doing that ordinary data can’t?

5. To what extent is Big Data currently being used for law enforcement and security intelligence in Canada?

6. Do you think Canadian agencies access to data and analytical tools is better or worse than (a) their foreign counterparts and (b) the private sector?

7. (a) In your view should this use by Canadian agencies be expanded?
   (b) If so, in what way should this be expanded and what could be achieved?
   (c) If not, why not, and what would be the implications?

8. (a) What do you see are the opportunities or possibilities that Big Data can open up for law enforcement and security intelligence?
   (b) How can these possibilities be delivered?
   (c) What are the barriers and how could they be overcome?
Big Data – Regulation

9. (a) What are the challenges and risks of Big Data technology to support law enforcement and enhance national security?
   (b) Who is exposed to these risks?
   (c) How should these challenges and risks be managed?

10. As you know, there are laws, regulations, guidelines and procedures governing the use of data by law enforcement or security agencies, including mechanisms for accountability and oversight.
    a. What laws, regulations, guidelines and procedures do you think are the most important in governing the collection and use of data for law enforcement and national security purposes? (Ask if we can obtain copies if possible, or find out where they are located)? Do any of these regulate Big Data techniques as such?
    b. In your view are these laws, regulations, procedures, guidelines (including oversight and accountability mechanisms) appropriate and effective?
    c. In particular, what do you think these are meant to achieve and do you feel they are successful?
    d. What are the shortcomings of the current laws, regulations, guidelines and procedures (including oversight and accountability mechanisms)? How do you think they should be changed?
    e. What other regulatory or management strategies are required for Big Data?
    f. [This question only relevant for those who, in answering questions above, were sceptical about capacity of Big Data] Assuming that Big Data had been proven effective in other instances, are there ways that Big Data techniques could be used appropriately? What kind of laws, regulations, accountability mechanisms would need to be in place?

11. [If appropriate] Do you have a sense of the history of these regulations? If yes, why are they the way they are?

12. What protections, if any, should remain in place in circumstances where an individual consents to the use or sharing of their data?

Scenario:

13. Now I would like to ask you a series of questions in relation to a hypothetical scenario:

   (Show card)

   Lucy is an 8 year old girl who has been kidnapped from her home in Ottawa. All avenues of traditional physical surveillance and canvassing of the area so far haven’t produced any leads.

   How do you feel about the immediate and expeditious use of big data tools in these circumstances?

   Probe further if necessary:
   - Metadata search of all known kidnappers with previous arrests in the area matched against CCTV footage from public and private sources in the area on the day of the kidnapping
• Collection of data and monitoring of all known kidnappers (with previous arrests) including known addresses, registered telephonic devices, social media accounts, email accounts,

• Facial recognition deployed on CCTV footage across all Ottawa and surrounding areas, and across multiple social media networks in an attempt to identify Lucy

• Metadata from all devices of all family members of Lucy, her neighbours, and people seen visiting the house that day (postal worker, Fedex, water meter inspection, etc.)

*What difference would it make if this was not just a kidnapping but there's suspicion of paedophilia?*

*What difference would it make if there was suspicion that the kidnapping was linked to terrorism, with an intent to blow Lucy up in a public place?*

14. To what extent should considerations such as privacy give way in the face of serious, imminent threats such as child kidnapping, child sexual abuse or terrorism?

15. To what extent should there be public transparency about

   (a) the nature of data collected or

   (b) the algorithms employed in analysis?

   (c) To what extent should there be intra-agency or intra-government transparency about these two things?

16. (a) How do you think your / your organisation’s views about the design and regulation of Big Data technology align with the views of other stakeholders?

   (b) Do you have any thoughts on how any conflict might be resolved?

17. To what extent are your views shaped by internal or personal experience as opposed to external sources such as blogs, watch groups and media?

*Thank you very much for taking the time to be interviewed. Your input is much appreciated*