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

January 28, 2014

Office of the Privacy Commissioner of Canada
112 Kent Street
Ottawa, Ontario
K1A 1H3

IP54-55/2014E-PDF
978-1-100-23180-8

Follow us on Twitter: @PrivacyPrivee

Contents

Introduction: Mandate of our Office and the Purpose of this Report

The last few months have seen intensified concerns about the protection of privacy in the context of national security activities. In order to contribute to an informed, constructive debate to address these concerns, the Office of the Privacy Commissioner of Canada (OPC) has produced this report in the hope of assisting Parliament in addressing the question as to whether Canada still has proper privacy protection in the context of national security.

The OPC oversees compliance with both the *Privacy Act*, governing the federal public sector, and the *Personal Information Protection and Electronic Documents Act*, governing the private sector. Intelligence organizations and operations are subject to the *Privacy Act*, which applies to the personal information practices of federal institutions to ensure that the privacy of individuals is protected.[1]

[1] *Privacy Act*, R.S.C., 1985, c. P-21, section 2.

The Privacy Commissioner of Canada is an independent Agent of Parliament. The OPC takes complaints, conducts audits and provides advice on privacy issues to commercial organizations, federal government institutions and Parliament. This special report is tabled before both Houses, pursuant to section 39(1) of the *Privacy Act*.

While the OPC oversees the entire public service for compliance with the *Privacy Act*, specialized bodies were created to handle compliance and review, including privacy, of intelligence operations in Canada: the Security Intelligence Review Committee (SIRC), the Office of the CSE Commissioner (OCSEC) and the Commission for Public Complaints against the RMCP (CPC).

The right to privacy is fundamental in Canada. It is central to personal integrity and essential to a free and democratic society. Recent events have brought to light new privacy risks within the current political and technological framework of intelligence activities. The evolution of security threats to open, democratic states - combined with the speed and power of technical surveillance practices and the desire to prevent or prepare for attacks of violence - create a pressing issue for democratic states to confront. As public concerns mount with regard to privacy protection in this context, the purpose of this report is to offer concrete recommendations and further a reasonable, constructive public debate.

How has the National Security Context Changed?

It is important to highlight the impact of political and societal changes that affect intelligence work and privacy today.[2] Broadly speaking, Canadian security experts have summarized these shifts as follows:

- The traditional divide between domestic and foreign threats has been eroded with global trends in international migration and expanded use of Internet tools. For example, Canadian citizens have participated in terrorist attacks abroad;
- The technical capacity for surveillance has grown exponentially, enhanced by the unprecedented creation and sharing of open-source personal information online. For example, national security agencies use personal information from social network sites;
- The very exchange of personal information itself generates still more personal information through profiles and metadata. Specifically, online communications create data trails that can paint a detailed picture of individuals;
- National security threats, traditionally attached to specific adversarial states such as the Soviet Union during the Cold War, have become pluralized and dispersed. For example, some individuals, as part of the general population, have become radicalized and may pose a threat to national security;
- With surveillance capacity increasing, thanks to new technologies and tools, far greater scales of collection are possible. For example, closed circuit televisions have become ubiquitous;
- Meanwhile, individuals who pose a threat themselves exploit personal information to further their own ends. For example, the use of stolen identities and communicating by the Internet.

[2] Angela Gendron and Martin Rudner, Assessing Cyber Threats to Canadian Infrastructure (March 2012) – URL: http://publications.gc.ca/collections/collection_2013/scrs-csis/PS74-1-2012-eng.pdf, pp. 21-34. See also Martin Rudner, "Canada's Communication Security Establishment: From Cold War to Globalization," Centre for Security and Defence Studies Occasional Paper, no. 22 (2000) – URL: http://circ.jmellon.com/docs/pdf/canadas_communications_security_establishment_from_cold_war_to_globalization.pdf, pp. 23-34; Special Senate Committee on Anti-Terrorism. *Security, Freedom and the Complex Terrorist Threat* (2011) – URL: http://www.parl.gc.ca/content/sen/committee/403/anti/rep/rep03mar11-e.pdf, pp. 9-22.

What has been the Impact on Privacy?

The critical impact of these changes upon privacy comes from the unprecedented importance and availability of personal information. Intelligence activities are now turned towards individuals dispersed within the general population.[3] As a result, the manner of conducting those activities can cast a wide net. Open source information such as that found on social networking sites is swept up electronically and has the potential to become the predominant collection channel. However, information online is often shared with an expectation of privacy – whether that is reasonable to expect or not – and moreover, can be inaccurate. As other commentators have remarked, the Internet has eradicated neat territorial distinctions, sectorial boundaries and jurisdictional remits when it comes to data collection, information sharing and intelligence analysis, while amplifying intelligence gathering capacity by orders of magnitude.[4] Moreover, the private sector, namely, the telecommunications sector, is therefore increasingly tasked directly with intelligence gathering or exploited for those purposes. Canada's intelligence agencies have been drawn increasingly into domestic domains (e.g. to combat local radicalization or financial sponsorship of violent movements).

The potential for intrusion upon privacy within this new context is such that it calls for commensurate privacy protection.

[3] Rudner, Martin, "Canada's Communications Security Establishment, Signals Intelligence and counter-terrorism" from Intelligence and National Security, 22:4 (2007), pp. 473-490.
[4] Wright, Andrea, "Security Intelligence: New Challenges for Democratic Control" (2007) for 2007 European Consortium for Political Research (ECPR) Conference.

Specific Accountability Challenges in the Intelligence Context

SECRECY AND ACCOUNTABILITY

While secrecy may be an inherent aspect of many intelligence activities, so is accountability. Reporting, review and appropriate legal controls lead to accountability on the part of decision-makers and institutions. National security claims do not reduce accountability obligations and security bodies must account to Canadians for what they do with personal information.[5] Independent review mechanisms ensure this accountability of security agencies, safeguard public trust and verify demonstrable respect for individual rights.[6]

As the former CSE Commissioner, the Honourable Robert Décary noted in his last annual report for 2012-2013, "much remains to be done, but I believe that the ice has been broken and that the security and intelligence agencies understand they can speak more openly about their work without betraying state secrets or compromising national security. The greater the transparency, the less sceptical and cynical the public will be." Transparency is key to accountability.

That said, in many instances the personal details on employees, paid informants, targets and persons of interest must remain protected. There are reasonable limits to complete and proactive disclosure of all government operations, particularly those engaged in a security and intelligence function. Sources and techniques should not be divulged if they are to remain effective and reliable. Highly-sensitive operational exchanges with other governments and partners must be undertaken with some measure of confidence and cannot be elaborately described. However, it is important to note that provisions to safeguard information in these cases are already provided for in existing law: the *Canadian Security Intelligence Service Act*, *Security of Information Act*, *Canada Evidence Act*, *Privacy Act* and *Access to Information Act*.[7]

Security bodies themselves would benefit from greater public discourse, where they must be able to engage in an intelligent discussion on the primary issues of privacy, at a minimum. Intelligence organizations have traditionally eschewed public debate about their roles in democratic societies. Their appearances in open proceedings of the legislature have been relatively few. Canada is by no means unique; this culture of secrecy has held fast for almost sixty years among all our allies. However, both CSEC and OCSEC have recently added new information to their websites to address issues of public concern, current media

[5] Deibert, Ronald, "Bounding Cyber Power: Escalation and Restraint in Global Cyberspace" CIGI Internet Governance papers (October 2013) – URL: http://www.cigionline.org/sites/default/files/no6_2.pdf, p. 15; also Deibert, Ronald, *Black Code: Inside the Battle for Cyberspace* (2013), pp. 8-11, 31-43.

[6] Standing Senate Committee on National Security and Defence, "Lack of Oversight," from *Canadian Security Guide Book* (December 2004) – URL: http://www.parl.gc.ca/Content/SEN/Committee/381/defe/rep/rep03nov04part2-e.htm#_Toc89252275

[7] Cohen, Stanley. *Privacy, Crime and Terror: Legal Rights and Security in a Time of Peril* (Lexis Nexis, 2005), pp. 289 – 314.

controversies and increase understanding of their work.

COOPERATION AMONG INTELLIGENCE AGENCIES WITHOUT COOPERATION AMONG REVIEW BODIES

As SIRC's most recent report notes, "the once-solitary worlds of Human Intelligence (HUMINT) and Signals Intelligence (SIGINT) have increasingly merged" and the increased integration of these domains can result in "erosion of control over the information shared." The Honourable Robert Décary noted in his last report that "where CSEC and CSIS cooperate and conduct joint activities, my office and SIRC do not have an equivalent authority to conduct joint reviews." He mentions, further, "I believe a certain amount of collaboration among review bodies is possible under existing legislation."

However, the *Privacy Act* remains essentially unrevised since 1983. Under the legislation, there are no provisions for joint audits or investigations with other like bodies, even in an era where information-sharing has increased greatly.

Survey of Oversight and Review Models for Intelligence Agencies

How do we achieve a high standard of privacy protection in this new intelligence context?

An overview of the United Kingdom, United States and Canadian models demonstrate the range of mechanisms that may be useful to consider.

UNITED KINGDOM

- In the UK, an independent Commissioner reviews warrant applications and approvals of government investigators under specific conditions sets out in statute.
- Statistics on interceptions of private communications undertaken are also compiled and reported annually, in addition to details on all government requests for so-called 'subscriber data' which can be used to identify particular individuals in an investigation. This regime has been operating since *Regulation of Investigatory Powers Act* (RIPA) was enacted in 2001.
- There are also special Commissioners established for data protection, surveillance, use of closed-circuit television (CCTV) and the intelligence services.
- As well, the UK has a specialized, security-cleared committee drawn from both Houses of Parliament – the Intelligence and Security Committee – to oversee national security activities with Ministerial approval (as revised under the 2013 *Justice and Security Act*).[8]

UNITED STATES

- In the US, a specially nominated bench of security-cleared justices preside over the Foreign Intelligence Surveillance Court (FISC), which approves both appropriate Federal Bureau of Investigation (FBI) and National Security Agency (NSA) surveillance activities.[9]
- Congress has a separate security cleared standing committee in each House specifically tasked with intelligence oversight. Both of these venues have been judged to provide an important challenge function.[10]

---

[8] United Kingdom, Parliament. A Bill to provide for oversight of the Security Service, the Secret Intelligence Service, GCHQ and other activities relating to intelligence or security matters; to provide for closed material procedure in relation to certain civil proceedings; to prevent the making of certain court orders for the disclosure of sensitive information; and for connected purposes (*Justice and Security Act* 2013) – URL: http://services.parliament.uk/bills/2012-13/justiceandsecurity/stages.html. See also Nicholas A. MacDonald, "Parliamentarians and National Security in Canada," from *Canadian Parliamentary Review* (Winter 2011) – URL: http://www.revparl.ca/34/4/34n4_11e_MacDonald.pdf

[9] Kaiser, Frederick, "Congressional Oversight of Intelligence: Current Structure and Alternatives" from *Intelligence Oversight and Disclosure Issues* (Nova, 2010), pp. 1-27.

[10] *Protecting individual privacy in the struggle against terrorists: a framework for program assessment*, National Research Council of the National Academies (Washington, DC: National Academies Press, 2008) – URL: http://iis-db.stanford.edu/pubs/22285/Protecting_Individual_Privacy.pdf, pp. 166 – 184.

- Congress also operates and directs the independent Government Accountability Office.
- The White House has appointed a Privacy and Civil Liberties Oversight Board to advise the President and report to Congress on counter-terrorism, privacy and civil liberties.
- In the US, annual reports are also provided to Congress on the use of wiretap surveillance, pen registers, and trap and trace devices.

CANADA

- In Canada, Parliament passed the *Canadian Security Intelligence Service* (CSIS) *Act* in the early 1980s.[11] Under that law, threat definitions and investigatory limits are clearly established.[12]
- The Act also established SIRC to protect Canadians' rights and freedoms and ensure that CSIS operates legally and appropriately at all times.[13]
- SIRC also reports intermittently on the number of warrants issued or renewed.
- By law, detailed reports are tabled annually to Parliament for review on the use of electronic surveillance by federal law enforcement (as a statutory requirement under section 195 of the *Criminal Code*).
- Annual reporting is also required with particulars on other extraordinary powers like preventative arrest and investigative hearings.[14]
- The OCSEC has provided annual reports to the Minister of National Defence every year since 1997, which have been tabled in Parliament. The CSE Commissioner's role is to ensure CSEC complies with the law and takes measures to protect the privacy of Canadians.
- Since 1988, the Commission for Public Complaints against the RCMP (CPC) has fulfilled a similar role in review.[15]

[11] House of Commons Special Committee on the Review of the *CSIS Act* and the *Security Offences Act*, "In flux but not in crisis: a report of the House of Commons Special Committee on the Review of the *Canadian Security Intelligence Service Act* and the Security Offences", Ottawa: Queen's Printer for Canada, 1990, pp. 83-184.

[12] Hardy, Timothy S., "Intelligence Reform in the mid-1970s" from CIA Center for the Study of Intelligence Archive, vol. 20, no. 2 – URL: https://www.cia.gov/library/center-for-the-study-of-intelligence/kent-csi/vol20no2/pdf/v20i2a01p.pdf, pp. 10-13.

[13] Security Intelligence Review Committee, "About SIRC" (October 2012) – URL: http://www.sirc-csars.gc.ca/abtprp/index-eng.html

[14] Public Safety Canada, *Annual Report on the Use of Electronic Surveillance* – 2012 – URL: http://www.publicsafety.gc.ca/cnt/rsrcs/pblctns/lctrnc-srvllnc-2012/index-eng.aspx; Public Safety Canada, *Annual Report Concerning Recognizance with Conditions: Arrests without Warrant* – URL: http://www.publicsafety.gc.ca/cnt/rsrcs/pblctns/rrsts-wtht-wrrnt-2007-eng.aspx; Justice Canada, *Backgrounder: The Combating Terrorism Act – Investigative Hearings and Recognizance with Conditions Provisions* (April 2010) – URL: http://www.justice.gc.ca/eng/news-nouv/nr-cp/2010/doc_32499.html

[15] Recent changes to the *RCMP Act* mean the CPC will soon take on an expanded role in review and be able to carry out broader systemic investigations which may examine national security work in more detail.

Recommendations for Improvement

The aim of renewal in this area should be to protect privacy in a complex threat environment; oversee collection so that it is reasonable, proportionate and minimally intrusive; ensure appropriate retention and access controls (among both public and private actors); ensure accuracy of analysis; and control the scope of information requests and disclosures through specific safeguards, agreements and caveats.[16]

In formulating the following recommendations, we have drawn extensively from the historical experiences of Canada, the UK and the US.[17] In our view, the current Canadian system of intelligence oversight would operate better if fine-tuned to new operational realities.[18] Listed below are a series of potential measures we believe could reasonably improve the existing framework and ensure that individuals' rights are protected.

AUGMENT EXISTING REVIEW AND REPORTING MECHANISMS

1. **Require CSEC to proactively disclose annual statistics on cases where it assists other federal agencies with requests for interception:**
   - Under the *National Defence Act*, CSEC can assist federal law enforcement and security agencies, including investigations of Canadians. Regular, annual public reporting would be an improvement in this regard, similar to SIRC's *Annual Report* and Public Safety Canada's *Annual Report on the Use of Electronic Surveillance*.[19]
   - Where possible, CSEC could also make public more detailed, current information about mandates, operating protocols and other statistical information, in keeping with open government principles.

2. **Require CSEC to produce an annual report for the Minister to table in Parliament:**
   - Amend the *National Defence Act* to require CSEC to produce a non-classified public report to be tabled in Parliament, as CSIS does, describing its ongoing activities and a summary of its risk assessments (violent extremism, organized crime, foreign corruption, etc.) and general policy priorities.[20]

[16] Wright, Andrea, "Casting Light into the Shadows: Why Security Intelligence Requires Democratic Control, Oversight and Review", from *The Human Rights of Anti-Terrorism* (Irwin, 2008), pp. 327-370.
[17] Littlewood, Jez, "Accountability of the Canadian Security and Intelligence Community post 9/11: Still a Long and Winding Road?" from *Democratic oversight of intelligence services* (Federation, 2010), pp. 83-107.
[18] Forcese, Craig, "The Collateral Casualties of Collaboration: The Consequence for Civil and Human Rights of Transnational Intelligence Sharing" from *International Intelligence Cooperation and Accountability* (London: Routledge, 2011), pp. 72-97.

[19] Canada. Communications Security Establishment, "Inside CSE: Assistance to federal law enforcement and security agencies" (December 2013) – URL: http://www.cse-cst.gc.ca/home-accueil/inside-interieur/assist-assistance-eng.html
[20] Many of these details are described in other CSEC publications routinely made public or released through the access to information process.

3. **Extend existing reporting requirements on use of surveillance:**
   - Report other forms of electronic monitoring and surveillance where national security is the basis for authorization in Public Safety Canada's *Annual Report on the Use of Electronic Surveillance*. This can include use of production orders, location tracking and installation of data recorders available to investigators under the *Criminal Code*.
   - For reporting purposes, separate domestic and foreign mandated activities, as well as those activities that require approval through warrants versus "non-warrant" investigatory aids.

4. **Update the overview of Canada's Intelligence Community:**
   - Refresh and re-issue the *Canadian Security and Intelligence Community* overview for public awareness and media reference, issued last in 2001 by the Intelligence Secretariat at PCO.[21]
   - Describe the underlying process of intelligence gathering and collection in the overview, explaining how intelligence priorities and requirements are set, and indicate what internal controls exist within the security and intelligence apparatus in Canada.[22]
   - Request from the government production of a White Paper on clarification of mandates in Canada's intelligence community and how they cooperate with global partners. The importance of privacy and the *Canadian Charter of Rights and Freedoms*, as well as lessons learned from various Commissions of Inquiry (O'Connor, Iacobucci and Major) should also be addressed in the terms of reference.[23] Once released, the document could aid deliberation and longer term improvements.

5. **Report on the Recommendations of the Major Commission of Inquiry:**
   - Provide a public status report (as requested by Justice Major at the end of his mandate as Commissioner of Inquiry) on consideration, rejection or implementation of his recommendations, as well as those of the 2006 O'Connor Policy Review.[24]

---

[21] Privy Council Office, *Canadian Security and Intelligence Community* (2001) – URL: http://www.pco-bcp.gc.ca/docs/information/publications/aarchives/csis-scrs/pdf/si-eng.pdf

[22] For example, some justification is needed to explain how signals intelligence collection priorities are currently set, given that internal controls on collection at CSEC are minimal (unlike the internal targeting processes at CSIS) and have no judicial review (as RCMP or CBSA do). Greater access to information about the functioning of the national security apparatus and the personal information that agencies collect and analyze is essential to ensure effective democratic control and debate. See Federal Court of Canada, Redacted amended further reasons for order in the matter of an application by XX for a warrant pursuant to sections 12 and 21 of the *Canadian Security Intelligence Service Act*, R.S.C. 1985, c.-23, 2013 FC 1275 – URL: http://reports.fja.gc.ca/eng/2015/2013fc1275.html

[23] Privy Council Office, Securing An Open Society: Canada's National Security Policy (2004) – URL: http://publications.gc.ca/site/eng/259263/publication.html, p. 19.

[24] Greater clarity for citizens and Parliament around how operational reviews have been undertaken in the past, and what lessons were learned (e.g. RCMP internal review post-O'Connor) should also be a priority. Some form of public engagement and consultation should also be brought to the Privy Council Office (PCO) requirements process to ensure openness with regard to setting intelligence priorities. From the Commissioner of Inquiry into the Investigation of the Bombing of Air India Flight 182, in this particular context, those recommendations arising from volume 4, entitled the Unique Challenges of Terrorism Prosecutions: Towards a Workable Relation between Intelligence and Evidence (2010) – URL: http://publications.gc.ca/collections/collection_2010/bcp-pco/CP32-89-5-2010-4-eng.pdf, pp. 204-311.

MODERNIZE OUR PRIVACY PROTECTION REGIME

6. **Reform existing privacy legislation to curb over-collection and control disclosure:**
    - Amend both federal privacy laws, the *Privacy Act* and *Personal Information Protection and Electronic Documents Act* (PIPEDA).[25]
        - Specific to this context, under the *Privacy* Act, require government departments to demonstrate the necessity for collecting personal information.
        - Require Privacy Impact Assessments prior to implementing new programs.
        - Strengthen the provision relating to the exchange of personal information with foreign authorities to promote privacy. In particular:
            - Canadian agencies should exercise the greatest care with personal information they pass to foreign agencies.
            - They have a duty to ensure the investigative foundation of any information they pass on.
            - Caveats must also be attached as to the use and dissemination of sensitive information among domestic agencies and foreign entities.
            - Rules for cooperation between domestic and foreign agencies must be as clear as possible beforehand and where practical reduced to writing.
            - Canadian agencies must be careful in labelling persons.
            - Canadian agencies cannot recycle imported intelligence without assessing its accuracy.
    - Expand the grounds for recourse to the Federal Court under the *Privacy Act*. Currently, our Office can only bring to the Federal Court matters relating to access to one's personal information. While the SIRC and the CSE Commissioner have the right to take complaints from the public, our Office may receive complaints about national security issues outside their jurisdiction. If these concern collection, use and disclosure, we have no recourse to Federal Court except in relation to access to personal information. Consequently, we recommend the grounds for Federal Court review be expanded to cover collection, use and disclosure of personal information.
    - Similarly, require public reporting on the use of various disclosure provisions under PIPEDA where private-sector entities such as telecommunications companies release personal information to national security entities without court oversight.
    - While oversight for privacy protection in the national security context is divided among more than one oversight body, the *Privacy Act* does not allow the OPC to cooperate with the other bodies. The Act should be amended to enable cooperation.

[25] As mentioned above, intelligence collection and analysis capacities are more engaged across sectors and borders than ever before, while the roles for review bodies and Parliamentary engagement have remained largely static.

7. **Regulate access to open-source information and investigations exploiting publically available personal information sources**
   - 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.

STRENGTHEN THE CURRENT ACCOUNTABILITY REGIME

8. **Bolster the powers of the federal bodies reviewing national security operations:**
   - Concretely address past OCSEC, CPC and SIRC concerns with respect to the conduct of joint reviews, with advance consultation with each body on necessary measures.[26]

9. **Clarify and update other legal authorities in intelligence operations:**
   - Clarify the provisions in the *National Defence Act* (NDA) for Ministerial Authorization to circumscribe CSEC activities at the statutory level. As previously recommended, statutory definitions for "activity", "class of activities", "intercept" and "interception" would be welcomed.[27]
   - Review the CSEC mandates set out in legislation and make the broader terms, references and definitions for their operations explicit in the NDA.[28]

---

[26] For example, Office of the CSE Commissioner, *Current Issues: Questions and Answers* (January 13, 2014) – URL: http://www.ocsec-bccst.gc.ca/new-neuf/faq_e.php

[27] OCSEC, *2007-2008 Annual Report* (2008) – URL: http://www.ocsec-bccst.gc.ca/ann-rpt/2007-2008/ann-rpt_e.pdf; *2009-2010 Annual Report* (2010) – URL: http://www.ocsec-bccst.gc.ca/ann-rpt/2009-2010/ann-rpt_e.pdf; *2012-2013 Annual Report* (2013) – URL: http://www.ocsec-bccst.gc.ca/ann-rpt/2012-2013/ann-rpt_e.pdf.

[28] Hubbard, Brauti, Fenton. "Electronic Surveillance under the *National Defence Act*" from Wiretapping and Other Electronic Surveillance: law and Procedure (March 2008), 17-1 – 17-10; Penney, Steven. "National Security Surveillance in an Age of Terror: Statutory Powers & Charter Limits." Osgoode Hall Law Journal 48.2 (2010): 247 – URL: http://digitalcommons.osgoode.yorku.ca/ohlj/vol48/iss2/2

10. Increase coordination of and investment in Parliament's oversight role:

The foregoing does not preclude a greater role for Parliamentarians. In general terms, it remains Parliament's role to seek accountability to Canadians.[29] To that end we recommend that Parliamentarians:

- Conduct a global study of the state of Canada's intelligence oversight and review mechanisms. Existing Parliamentary venues can address political and Ministerial accountability while also producing useful studies and raising policy questions;[30]
- Regularly call representatives of the Canadian intelligence community to appear before committees;
- Hear from civil society, advocates and academics working in this area; and
- Coordinate their topics for study and witnesses to enhance coverage of the Canadian intelligence community. For example, it could be of great value for Parliamentarians to examine privacy issues in light of the emergent interface between security agencies, private sector stakeholders and the need to safeguard critical infrastructure.

[29] Interim Report of the Special Senate Committee on Anti-Terrorism. Security, Freedom and the Complex Terrorist Threat (March 2011) – URL: http://www.parl.gc.ca/content/sen/committee/403/anti/rep/rep03mar11-e.pdf, pp. 42-46.

[30] Canada. Commission of Inquiry Concerning Certain Activities of the Royal Canadian Mounted Police, *Second Report: Freedom and Security under the Law* (1981) – URL: http://epe.lac-bac.gc.ca/100/200/301/pco-bcp/commissions-ef/mcdonald1979-81-eng/mcdonald1979-81-report2/mcdonald1979-81-report2-vol2-eng/mcdonald1979-81-report2-vol2-part2-eng.pdf, pp. 891-905.

Conclusion: Privacy as Part of Intelligence Oversight

As the Office of the Auditor General reminded us in its report of March 2009, “for Canadians to have confidence in their security and intelligence organizations, they need to know that government agencies and departments maintain a balance between protecting the privacy of citizens and ensuring national security.”[31]

We hope this report can aid that effort.

[31] Office of the Auditor General of Canada, *2009 March Report of the Auditor General of Canada – Chapter 1 – National Security: Intelligence and Information Sharing*; p. 2.

Acknowledgements

Our Office would like to single out for special thanks the two lead advisors on the research and review phase of the project: Martin Rudner (Distinguished Research Professor Emeritus, Norman Paterson School of International Affairs at Carleton University) and Ray Boisvert (Chief Executive Officer I-Sec Integrated Strategies (ISECIS) and retired Assistant Director of Intelligence, CSIS). Their insights and understanding were critical contributions throughout the process.

Also we are grateful for the insights offered by a dedicated group of practitioners: Robert Marleau (former Clerk of the House of Commons, interim Privacy Commissioner and Information Commissioner of Canada), Horst Intscher (former head of Financial Transactions and Reports Analysis Centre of Canada), Angela Gendron (Senior Fellow at the Canadian Centre of Intelligence and Security Studies, Carleton University) and Dave McMahon (Chief Operations Officer, Sec Dev Group) – as each contributed their time and energy in reviewing the ideas and proposals set out in the report.

Finally, we provided the report for comment to stakeholder organizations working in the space of security review and civil liberties. These included the Commission for Public Complaints against the RCMP (CPC), Canadian Civil Liberties Association (CCLA) and the International Civil Liberties Monitoring Group (ICLMG). There was considerable difference of opinion but we would like to recognize each for their clarifications, comments and criticisms.

Appendix A: Historical Summary of Past OPC Recommendations on Oversight, Controls and Privacy Protections for Intelligence Activities

In 2005, our Office tabled a set of recommendations for strengthening oversight and privacy protection in the case of CSEC as the House of Commons conducted its review of the *Anti-terrorism Act*. In 2008, following the reports of the O'Connor and Iacobucci Inquiries, we made a case to Parliament for reforming the *Privacy Act* in light of intensified intelligence sharing and surveillance activities on the part of national security agencies. In 2009, at the invitation of the House Standing Committee on Public Safety and National Security, we recommended various mechanisms for treating intelligence oversight gaps that we had observed. In 2011, in a submission to government consultation on perimeter security and greater intelligence cooperation with the US, we put forward a set of recommendations on surveillance and monitoring. Most recently, in 2013, we argued for improvements to transparency and accountability when private sector firms supply personal information to government for law enforcement purposes. All these were included in public submissions:

From *OPC Submission on the Anti-terrorism Act* - May 9, 2005 (http://www.priv.gc.ca/parl/2005/ata_050509_e.asp#section4.2)

- The *Anti-terrorism Act*'s amendments to the *National Defence Act* to allow the Communications Security Establishment to intercept private conversations that may involve people in Canada should be amended to require prior judicial authorization.
- Section 273.65(2)(d) of the *National Defence Act,* which purports to protect the privacy of Canadians in the face of CSE surveillance of communications, should be amended. The requirement for "satisfactory measures... to protect the privacy of Canadians and to ensure that private communications will only be used or retained if they are essential to international affairs, defence or security" should be amended, either to require "all reasonable measures to protect privacy" or to specify in greater detail what constitutes "satisfactory" measures.
- Section 273.65(4)(d) of the *National Defence Act*, which permits CSE to collect information essential to protecting the government's computer systems, places limitations on what can be "used" and "retained". This should be amended to place limitations on what information CSE can obtain.
- Section 273.65(8) of the *National Defence Act* should be amended so that the CSE Commissioner is required to ensure not only that intercepts of private conversations have been authorized by Ministerial direction, but that the direction itself is authorized by the law and consistent with the *Canadian Charter of Rights and Freedoms* and the *Privacy Act*.

From *Government Accountability for Personal Information: Reforming the Privacy Act* - April 2008 (http://www.priv.gc.ca/information/pub/pa_ref_add_080417_e.asp)

- Create a legislative requirement for government departments to demonstrate the necessity for collecting personal information.
- Broaden the Federal Court review to all grounds under the Privacy Act, rather than being limited to denial of access as is currently the case.
- Enshrine into law the obligation of Deputy Heads to carry out Privacy Impact Assessments prior to implementing new programs and policies, including a requirement to submit the PIA for review by the OPC, and requiring public disclosure of PIA results, subject to national security constraints.
- Enunciate a clear public education mandate.
- Provide greater flexibility for the OPC to publicly report on the government's privacy management practices, rather than being limited to the current mechanisms of annual and special reports.
- Provide discretion for the OPC to more efficiently and expeditiously deal with complaints which have less systemic and societal significance, enabling the OPC to invest more resources in complaints that will have a significant impact on improving the state of personal information management across the federal government.
- Align the *Privacy Act* with PIPEDA by eliminating the restriction that the *Privacy Act* applies only to recorded information.
- Strengthening the annual reporting requirements under section 72 of the *Privacy Act*, to require government institutions to report to Parliament on a broader spectrum of privacy management responsibilities, including those under Treasury Board policies on Privacy Impact Assessments and Data Matching.

From *Rights and reality: enhancing oversight for national security programs in Canada* – May 2009 (http://www.priv.gc.ca/parl/2009/parl_sub_090507_e.asp)

- Reiterate the importance of integrating the approach of existing review bodies to allow for more coordination and cooperation on reviews and reports across the system. Joint investigations and collaborative reporting with federal review bodies have worked to great effect in the experience of the OPC and all government operations would benefit.
- Address privacy and data management within agencies. Both the O'Connor and Iacobucci Inquiries focused on how information was shared and the quality of that information. Enhanced training around the theory and practice of privacy, fair information practices and data protection could effect great change.
- Urge appointment of Chief Privacy Officers across government –in particular to agencies where collection of sensitive personal information is widespread.
- Provide the Commission for Public Complaints against the RCMP with the resources and legal authorities required to exercise more meaningful review.
- Emphasize the urgency of the Treasury Board and Ministers issuing new policy requirements for departments and agencies to use Information Sharing Agreements, conduct Privacy Impact Assessments and develop privacy direction and guidance.
- Urge government to move on reform for *the Privacy Act*.

- Increase Parliament's role in national security oversight. Given the critical importance of the file, additional resources and involvement of this House Committee and its counterpart in the Senate to review national security agencies is needed. By pooling expertise, coordinating reviews and sharing information, existing mechanisms could be augmented.

From *Fundamental Privacy Rights within a Shared Vision for Perimeter Security and Economic Competitiveness* – June 2011 (http://www.priv.gc.ca/information/research-recherche/sub/sub_bs_201106_e.asp)

- Establish clear controls and limits on information-sharing: While the final reports of the O'Connor Inquiry made many recommendations to treat issues within the RCMP, the pivotal importance of constraints, controls and caveats on information and intelligence sharing cannot be overstated.
- Expand oversight and challenge functions in cross-border intelligence analysis: the OPC would caution strongly against any arrangements where care and custody of personal information is unclear or weak accountability are in place for use outside of Canada.
- Privacy impact assessment (PIA) processes should be applied
- Increase privacy safeguards for cross-border data exchange: provisions in the federal Privacy Act governing the disclosure of personal information by the Canadian government to foreign states must be strengthened.
- Reinforce the foundational protection and respect of rights and freedoms online: Cooperation and intelligence-gathering by government in the context of cyber security should not expand to the detriment of individuals' privacy, civil liberties and constitutional guarantees. Canada and the US should enter into discussions on cyber security cooperation with this risk in mind.
- Avoid purely technical solutions and strategies: Any shared effort must be accompanied by clear legal guidance, expanded education and public awareness around data security and information protection practices, stronger efforts to support independent, multidisciplinary research on cyber issues, bi-national commitment to developing better protective, privacy enhancing security standards, and ensuring regulatory bodies have the capacity and authorization to ensure better industry practices.
- Broaden public consultation, dialogue, education and outreach: In this digital age, where citizens expect engagement and interaction, that lack of open dialogue is clearly unacceptable and will undermine long-term efforts. Both Canadian and US officials need to create mechanisms for regular public reporting, engagement and an open process to hear concerns and complaints as they begin cooperative cyber security efforts.
- Expand public research and dialogue into the international challenges in cyber security efforts: Much more involvement from academics, civil society, media and individual citizens is needed. Universities in Canada and across the US should be encouraged to develop focus and expertise and to establish networks and joint events to share their research. Open sourcing, open discussion and open debate on cyber security and infrastructure protection issues should be the norm, not the exception.

From *The Case for Reforming the Personal Information Protection and Electronic Documents Act* - May 2013 (http://www.priv.gc.ca/parl/2013/pipeda_r_201305_e.asp)

- Lift the veil on authorized disclosures- Require organizations to publicly report on the number of disclosures they make to law enforcement under paragraph 7(3)(c.1), without knowledge or consent, and without judicial warrant, in order to shed light on the frequency and use of this extraordinary exception.

Sources

- Baldino, Daniel, ed. *Democratic oversight of intelligence services* (Sydney: The Federation Press, 2010).
- Ball, Kirstie; Haggerty, Kevin D.; Lyon, David, eds. *Routledge handbook of surveillance* (New York, NY: Routledge, 2012).
- Born, Hans and Caparini, Marina. *Democratic Control of Intelligence Services: Containing Rogue Elephants* (Burlington, VT: Ashgate Publishing Co, 2007).
- Born, Hans; Leigh, Ian; Wills, Aidan (Eds.) *International Intelligence Cooperation and Accountability* (London: Routledge, 2011).
- Canada. Commission of Inquiry Concerning Certain Activities of the Royal Canadian Mounted Police. *Certain R.C.M.P. activities and the question of governmental knowledge: third report* (Ottawa: The Commission, c1981) – URL: http://epe.lac-bac.gc.ca/100/200/301/pco-bcp/commissions-ef/mcdonald1979-81-eng/mcdonald1979-81-eng.htm
- Canada. Commission of Inquiry Concerning Certain Activities of the Royal Canadian Mounted Police. *Freedom and security under the law: second report* (Ottawa, 1981) – URL: http://epe.lac-bac.gc.ca/100/200/301/pco-bcp/commissions-ef/mcdonald1979-81-eng/mcdonald1979-81-eng.htm
- Canada. Commission of Inquiry Concerning Certain Activities of the Royal Canadian Mounted Police. *Security and information: first report* (Ottawa: Commission, 1979) – URL: http://epe.lac-bac.gc.ca/100/200/301/pco-bcp/commissions-ef/mcdonald1979-81-eng/mcdonald1979-81-eng.htm
- Canada. Commission of Inquiry into the Actions of Canadian Officials in Relation to Maher Arar. *A new review mechanism for the RCMP's national security activities* (Ottawa, 2006) - URL: http://epe.lac-bac.gc.ca/100/200/301/pco-bcp/commissions-ef/arar-ef/policy_review_report-e/PolicyReviewDec12-English.pdf
- Canada. Commission of Inquiry into the Actions of Canadian Officials in Relation to Maher Arar. *Report of the events relating to Maher Arar* (Ottawa, 2006) – URL: http://www.pch.gc.ca/cs-kc/arar/index_e.htm
- Canada. Office of the Communications Security Establishment Commissioner. *Annual Report* (June 2013) – URL: http://www.ocsec-bccst.gc.ca/ann-rpt/2012-2013/ann-rpt_e.pdf
- Canada. Privy Council Office. *Canadian Security and Intelligence Community* (2001) – URL: http://www.pco-bcp.gc.ca/docs/information/publications/aarchives/csis-scrs/pdf/si-eng.pdf
- Canada. Privy Council Office. *Report of the Interim Committee of Parliamentarians on National Security* (2004) – URL: http://www.pco-bcp.gc.ca/docs/information/publications/aarchives/cpns-cpsn/cpns-cpsn-eng.pdf
- Canada. Privy Council Office. *Securing an open society: Canada's National Security Policy* (Ottawa, 2004). – URL: http://publications.gc.ca/site/eng/259263/publication.html
- Canada. Security Intelligence Review Committee. "The Case for Security Intelligence Review in Canada" from *Reflections.: Twenty Years of Independent External Review of Security Intelligence in Canada* (Ottawa, 2005) – URL: http://www.sirc-csars.gc.ca/opbapb/rfcrfx/sc02a-eng.html

- Canada. Royal Commission on Security. *Report of the Royal Commission on Security* (Ottawa: Supply and Services Canada, 1969) - URL: http://epe.lac-bac.gc.ca/100/200/301/pco-bcp/commissions-ef/mackenzie1969-eng/mackenzie1969-eng.pdf
- Canada. Special Senate Committee on Anti-Terrorism. *Security, Freedom and the Complex Terrorist Threat* (March 2011) – URL: http://www.parl.gc.ca/content/sen/committee/403/anti/rep/rep03mar11-e.pdf
- Canada. Standing Senate Committee on National Security and Defence. *Canadian Security Guide Book* (December 2004) – URL: http://www.parl.gc.ca/Content/SEN/Committee/381/defe/rep/rep03nov04-e.htm
- Cappe, Mel. "Strengthening Democracy Through Effective Review," remarks to the International Intelligence Review Agencies Conference (Ottawa, Canada, May 29, 2012).
- Cohen, Stanley A. *Privacy, crime and terror: legal rights and security in a time of peril* (Markham: LexisNexis Butterworths, 2005).
- Cox, James. "Canada and the Five Eyes Intelligence Community" from *CDFAI Strategic Studies Papers* (2012) – URL: http://www.cdfai.org/PDF/Canada%20and%20the%20Five%20Eyes%20Intelligence%20Community.pdf
- Daniels, J. Patrick Macklem and Kent Roach (eds.) *Security of Freedom: Essays on Canada's Anti-Terrorism Act* (UTP, Toronto, 2001).
- Deibert, Ronald. *Black Code: Inside the Battle for Cyberspace* (2013).
- Deibert, Ronald. "Bounding Cyber Power: Escalation and Restraint in Global Cyberspace" *CIGI Internet Governance papers* (October 2013) – URL: http://www.cigionline.org/sites/default/files/no6_2.pdf
- Diffie, Whitfield and Landau, Susan. *Privacy on the line: the politics of wiretapping and encryption* (Cambridge, Mass. MIT Press, 2007).
- Forcese, Craig. "Canada's National Security Complex: Assessing the Secrecy Rules" *IRPP Choices*, vol. 15, no. 5, June 2009 – URL: http://www.irpp.org/assets/research/security-and-democracy/canadas-national-security-complex/vol15no5.pdf
- Gendron, Angela and Martin Rudner, *Assessing Cyber Threats to Canadian Infrastructure* (March 2012) – URL: http://publications.gc.ca/collections/collection_2013/scrs-csis/PS74-1-2012-eng.pdf,
- Gendron, Angela. "Just War, Just Intelligence: An Ethical Framework for Foreign Espionage," *International Journal of Intelligence and Counterintelligence*, Vol. 18, No. 3 (Autumn, 2005).
- Goold, Benjamin J. and Neyland, Daniel. *New Directions in Surveillance and Privacy* (Cullompton, UK: Willian, 2009).
- Great Britain. Parliament. House of Lords. Select Committee on the Constitution. *Surveillance: citizens and the state volume II : evidence* (London: 2007) – URL: http://www.publications.parliament.uk/pa/ld200809/ldselect/ldconst/18/18ii.pdf
- Haas, Philipp R. *Intelligence Oversight and Disclosure Issues* (New York, NY: Nova Science Publishers, 2009).
- Haggerty, Kevin D. eds. *Surveillance and Democracy* (Abingdon, Routledge, 2010).
- Hanks, Peter and John McCamus. *National security: surveillance and accountability in a democratic society* (Cowansville, QC: Yvon Blais, c1989).
- Harris, Victor H. Does intelligence oversight support or hinder counterinsurgency (COIN) and homeland defense operations? (Ann Arbor, MI: ProQuest LLC, 2010).

- Harris, Shane. *The watchers: the rise of America's surveillance state* (New York: Penguin Press, 2010).
- Hubbard, Brauti, Fenton. "Electronic Surveillance under the National Defence Act" from *Wiretapping and Other Electronic Surveillance: law and Procedure* (March 2008), pp. 17-1 – 17-10.
- Lefebvre, Stephane. "Canada's Intelligence Culture: an assessment" from *Democratization of Intelligence: Melding Strategic Intelligence and National Discourse* (National Defense Intelligence College, Washington DC, 2009) – URL: http://www.ni-u.edu/ni_press/pdf/Democratization_of_Intelligence.pdf, pp. 79-98.
- Lefebvre, Stephane. "Canada's Legal Framework for Intelligence" from *International Journal of Intelligence and Counterintelligence*, Vol. 23, No. 2, 2010, pp. 247-295.
- Leigh, Ian Leigh and Ian Lustgarten, *In from the cold: national security and parliamentary democracy* (Oxford: 1994).
- MacDonald, Nicholas A. "Parliamentarians and National Security in Canada" from *Canadian Parliamentary Review* (Winter 2011) – URL: http://www.revparl.ca/34/4/34n4_11e_MacDonald.pdf
- Mattelart, Armand. *The Globalization of Surveillance* (Malden, MA: Polity, 2010).
- National Research Council of the National Academies. *Protecting individual privacy in the struggle against terrorists: a framework for program assessment* (Washington, DC: National Academies Press, 2008) – URL: http://iis-db.stanford.edu/pubs/22285/Protecting_Individual_Privacy.pdf
- Obar, Jonathan A. and Clement, Andrew. "Internet Surveillance and Boomerang Routing: A Call for Canadian Network Sovereignty" – URL**:** http://ssrn.com/abstract=2311792
- Office of the Auditor General of Canada, *2009 March Report of the Auditor General of Canada*.
- Penney, Steven. "National Security Surveillance in an Age of Terror: Statutory Powers & Charter Limits." *Osgoode Hall Law Journal* (2010) : 247 – URL: http://digitalcommons.osgoode.yorku.ca/ohlj/vol48/iss2/2
- Petersen, Julie K. *Understanding surveillance technologies: spy devices, privacy, history & applications* (Boca Raton: Auerback Publications, 2007).
- Priest, Dana and Arkin, William M. *Top Secret America: The Rise of the New American Security State* (NY: Little, Brown and Company, 2011).
- Rudner, Martin, "Canada's Communication Security Establishment: From Cold War to Globalization," *Centre for Security and Defence Studies Occasional Paper*, no. 22 (2000) – URL: http://circ.jmellon.com/docs/pdf/canadas_communications_security_establishment_from_cold_war_to_globalization.pdf
- Rudner, Martin, "Canada's Communications Security Establishment, Signals Intelligence and counter-terrorism" *from Intelligence and National Security*, 22:4, pp. 473-490.
- Solove, Daniel J. *Nothing to hide: the false trade-off between privacy and security* (New Haven: Yale University Press, 2011).
- Walters, Gregory J. *Human rights in an information age: a philosophical analysis* (Toronto, University of Toronto Press, 2001).
- Whitaker, Reg; Kealey, Gregory S.; Parnaby, Andrew. *Secret service: political policing in Canada from the Fenians to Fortress America* (Toronto: University of Toronto Press, 2012).
- Wright, Andrea. "Security Intelligence: New Challenges for Democratic Control" / Andrea Wright, paper presented at the European Consortium on Political Research (September 2007).
- Wright, Andrea, "Casting Light into the Shadows: Why Security Intelligence Requires Democratic Control, Oversight and Review" from *The Human Rights of Anti-Terrorism* (Irwin, 2008), pp. 327-370.