Office of the
Privacy Commissioner
of Canada

Commissariat
à la protection de
la vie privée du Canada

Regarding Financial Monitoring Regime in Canada

Office of the Privacy Commissioner of Canada's Submission in Response to the Commission of Inquiry into the Investigation of the Bombing of Air India Flight 182

November 6, 2007
Ottawa, Ontario

Jennifer Stoddart
Privacy Commissioner of Canada

Table of Contents

Introduction

On May 1, 2006, an Order in Council was issued defining the terms of reference for the Commission of Inquiry into the Investigation of the Bombing of Air India Flight 182. The Honourable John C. Major, Q.C., was appointed Commissioner. One subject on which the Commissioner was to make findings and recommendations was whether Canada's existing legal framework provides adequate constraints on terrorist financing in, from or through Canada. The Office of the Privacy Commissioner was subsequently asked to submit its views on Canada's anti-terrorist financing framework, recent changes made to relevant legislation and the privacy implications for Canadians. The Office has provided several submissions to the Senate and Department of Finance on the subject.[1] Our present comments to this Commission draw largely from these materials.

Overview of financial monitoring regime in Canada

While federal officials responsible for financial monitoring could provide the Inquiry with more detailed insight into the entire process, we would like to present a general overview of Canada's financial monitoring regime as initially set-up to combat money laundering.

Since its inception in 2000, the Financial Transactions and Reports Analysis Centre of Canada (FINTRAC) has collected data from a broad range of "covered entities", including financial institutions, foreign exchange dealers, casinos, securities brokers, accountants, real estate companies and several other types of business. These entities *must* collect specified information and maintain detailed records on their clients' identities and transactions, *must* report any dealing involving $10,000 or more, and *must* report any transaction when *reasonable grounds to suspect* money laundering or terrorist financing arise. These reports are secret, and made *without* the knowledge or consent of the clients.

FINTRAC then analyzes this data along with information from other sources including commercially available databases, voluntarily provided information, law enforcement databases and/or information from other federal agencies. This information can then be passed on to law enforcement agencies, the Canada Revenue Agency, CSIS, Canada Border Services Agency or other government bodies provided there is "reasonable grounds to suspect" that the information would be relevant to investigating or prosecuting a money laundering or terrorist financing offence. Data would be disclosed to certain agencies only in instances where suspicion of terrorist-financing or money laundering also coincided with offences falling within their mandate. For example, Canada Revenue would only be informed in cases of money laundering and tax evasion, Citizen and Immigration would only be informed of cases involving terrorist-financing and fraudulent refugee claims, and so forth.

---

[1] *Review of the Proceeds of Crime (Money Laundering) and Terrorist Financing Act: Submission to the Standing Senate Committee on Banking, Trade and Commerce*. URL: http://www.privcom.gc.ca/information/pub/sub_ml_060621_e.asp
Bill C-25, An Act to amend the Proceeds of Crime (Money Laundering) and Terrorist Financing Act and the Income Tax Act and to make a consequential amendment to another Act: Submission to the Standing Senate Committee on Banking, Trade and Commerce. URL: http://www.privcom.gc.ca/parl/2006/sub_061213_e.asp
Submission in Response to Finance Canada's Enhancing Canada's Anti-Money Laundering and Anti-Terrorist Financing Regime consultation. URL: http://www.fin.gc.ca/consultresp/regime_23e.html
Submission of the Office of the Privacy Commissioner of Canada to the Senate Special Committee on the Anti-terrorism Act. URL: http://www.privcom.gc.ca/media/nr-c/2005/ata_050509_e.asp

In summary, the original scope of FINTRAC data collection was expansive, has continued to grow and has been on-going since 2000. According to the Centre's last Annual Report, 37.4 million transaction reports were housed on its servers.[2] As the scope of data collection has grown, one official from FINTRAC recently noted this database now adds another 15 million reports each year.[3] And as reported in 2004 by the Auditor General, monitoring has resulted in few successful prosecutions.[4] All this to say the Centre has compiled a detailed database on individual Canadians and their finances, maintaining these records for a decade or more in some cases.[5] And from this regime has come little discernable benefit.

Recent expansion of the FINTRAC regime

In December 2006, with the passage of Bill C-25, *An Act to amend the Proceeds of Crime (Money Laundering) and Terrorist Financing Act and the Income Tax Act and to make a consequential amendment to another Act*, reporting to FINTRAC was expanded still further. To quickly summarize, Bill C-25 widened Canada's financial monitoring regime in a number of ways:

- The types of businesses required to report broadened to include, for example, public notaries in some provinces, dealers in precious stones and metals, and real estate developers;
- The types of transactions triggering these reports expanded. For example, new provisions require reporting of *attempted suspicious* transactions, not just completed transactions;
- The "know your customer" and due diligence requirements were strengthened in several ways. Businesses are expected to take measures to verify identity in non-face-to-face transactions. Regulations will require this identity information be updated and greater efforts will be required for businesses to identify individuals when there are doubts about previously obtained data;
- Special emphasis will be put on monitoring "politically exposed foreign persons" and members of their families;
- A registration process, including the collection of specified information, will be introduced for money service businesses and foreign exchange dealers, with FINTRAC acting as registrar;
- In order to address concerns about charities being used to fund terrorist organizations the government is proposing to allow increased sharing of information between the Canada Revenue Agency and FINTRAC; and,
- The list of designated information that FINTRAC can disclose to law enforcement and intelligence agencies will be expanded.

---

[2] *Financial Transactions and Reports Analysis Centre of Canada Annual Report* (Ottawa, 2006), p. 20. URL: http://www.fintrac.gc.ca/publications/annualreport/2006/AR_E.pdf

[3] Mark Potter (Acting Deputy Director, Department of Finance, Financial Transactions and Reports Analysis Centre of Canada) in evidence before the Standing Committee on Finance, no. 75, 1st Session, 39th Parliament - March 29, 2007 (Ottawa), p. 10. URL: http://cmte.parl.gc.ca/Content/HOC/Committee/391/FINA/Evidence/EV2825716/FINAEV75-E.PDF

[4] Office of the Auditor General of Canada, *Report of the Auditor General to the House of Commons – Chapter Two: Implementation of the National initiative to Combat Money Laundering* (Ottawa, 2004), p. 6. URL: http://www.oag-bvg.gc.ca/domino/reports.nsf/html/20041102ce.html/$file/20041102ce.pdf

[5] *Proceeds of Crime (Money Laundering) and Terrorist Financing Act*, paragraphs 54(d) and (e), p. 38. URL: http://laws.justice.gc.ca/en/ShowFullDoc/cs/P-24.501///en

Privacy concerns on the expansion of financial monitoring

In short, recent changes expand the ***depth*** of Canada's anti-terrorist financing regime considerably. The number of organizations required to monitor and to collect information about their clients and customers will increase, the amount of personal information being recorded will expand, more transaction types will be subject to scrutiny and reporting, the number of people whose financial transactions will be scrutinized will be greater than ever. More personal information will be collected on clients and customers, and businesses will keep even more detailed records on Canadians.

The ***range*** of persons under scrutiny has grown. To illustrate, one area of concern is the additional scrutiny of "politically exposed foreign persons" *and their families*. This term is extremely broad and would capture large numbers of people: head of state, cabinet members, legislators, senior bureaucrats, ambassadors, senior military officers, heads of crown corporations, heads of government agencies, judges, political party leader or holders of *any* prescribed office or position.[6] The idea that individuals will be subjected to added surveillance, not even on grounds of suspicion, but owing simply to their position is alarming. In many cases, this will be in addition to security checks and other screening conducted prior to their appointments. Assuming other partner countries adopt similar measures, Canadian officials and their families with business abroad can expect to be monitored in a parallel fashion. Given the number of information sharing agreements that FINTRAC has with similar bodies in other countries, we are concerned this provision could be used as a back door for countries to monitor their own officials.

The ***scope*** of the regime has also been extended. The number of government agencies at home and abroad with access to this highly sensitive data has increased, with new information sharing provisions for agencies within Canada and similar foreign entities. FINTRAC can now share information with the Communications Security Establishment (CSE), the RCMP, CSIS, the Canada Revenue Agency, the Canada Border Services Agency and Citizenship and Immigration. We should note CSE is not an investigation or enforcement agency and, unlike the agencies mentioned above, it cannot use any information it receives from FINTRAC for enforcement purposes. CSE can, however, use this information to subject individuals to other forms of electronic surveillance. Intelligence obtained by CSE could then be disclosed to the RCMP, CSIS, foreign agencies or forwarded back to FINTRAC. We question the need for this, given the potential for self-perpetuating surveillance.

Finally, the ***rationale and duration*** for information sharing has also broadened beyond the original intent of the legislation. Originally conceived to tackle money laundering specifically, financial data in certain circumstances can be used to investigate and prosecute money-laundering, terrorist financing, tax evasion, false immigration claims and fraudulent charities.[7] The period of data retention has lengthened since legislation passed in 2000 from five, then ten, and now to fifteen years in some cases. [8]

---

[6] *Proceeds of Crime (Money Laundering) and Terrorist Financing Act*, sec. 9.3 (3) URL: http://laws.justice.gc.ca/en/ShowFullDoc/cs/P-24.501///en

[7] Bill C-22*, An Act to facilitate combating the laundering of proceeds of crime, to establish the Financial Transactions and Reports Analysis Centre of Canada and to amend and repeal certain Acts in consequence* (Second Session, 36th Parliament, 1999-2000) section 55 (3), a-d. URL: http://www2.parl.gc.ca/content/hoc/Bills/362/Government/C-22/C-22_4/C-22_4.pdf

[8] Ibid, section 54 (d); *Proceeds of Crime (Money Laundering) and Terrorist Financing Act*, paragraphs 54(d) and (e)

To summarize, these changes have broadened the coverage of a regime that was already sweeping, with little or no explicit rationale or additional consideration given to possible oversight or privacy safeguards. Other reviews of the legislation had found its scope more than adequate. A 2004 Auditor General's report concluded that "Canada now has a comprehensive strategy against money laundering and terrorist financing that is generally consistent with international standards." [9]

Privacy concerns on mandatory reporting by business

As stated, the regime as it was created in 2000 was already unprecedented in scope, in particular the degree to which business was required to act as a *de facto* agent of the state. While other government initiatives have required the private sector (e.g. airlines) to provide personal information to government for investigatory purposes, they have not been required to collect data *beyond* business purposes *solely* to provide it to government for monitoring and analysis.

Canada's financial monitoring regime is different. As it stands, regulations under the *Proceeds of Crime (Money Laundering) and Terrorist Financing Act* compel financial institutions, currency exchange dealers, even jewellers and real estate brokers to collect personal information over and above what is needed for business purposes, *judge* what is or is not suspicious behaviour and to report it. Failure to do so can translate into a heavy fine or jail term. In Canada, for very strong constitutional reasons, policemen and courts have traditionally made these kinds of assessments. In fact, C-25 has also expanded the range of FINTRAC powers and jurisdiction. From a pure collection and analysis role, the Centre will now also act as a registrar, have an enforcement arm and be able to mete out its own administrative monetary penalties (AMP) for non-compliance.[10] With fines as high as $2 million, private sector organizations will seek to minimize risk and likely over-report to ensure compliance, as recent cases in the US have demonstrated.[11]

In short, the PCMLTFA regime has created a mandatory reporting scheme allowing government to access personal information for investigatory purposes *without* judicial authorization and *without* satisfying the standard requirement of reasonable and probable grounds but *with* sharp penalties for organizations and individuals who fail to report. As Stanley Cohen (General Counsel, Department of Justice) remarked before a Senate Committee reviewing C-25, such a *mandatory* reporting of suspicious transactions tests the limits of constitutional authority in Canada. [12]

---

[9] Office of the Auditor General of Canada, *Report of the Auditor General to the House of Commons – Chapter Two: Implementation of the National initiative to Combat Money Laundering* (Ottawa, 2004), p. 1. URL: http://www.oag-bvg.gc.ca/domino/reports.nsf/html/20041102ce.html/$file/20041102ce.pdf

[10] *Financial Transactions and Reports Analysis Centre of Canada - Report on Plans and Priorities for the years 2007-2008 to 2009-2010* (Ottawa), p. 8. URL: http://www.tbs-sct.gc.ca/rpp/0708/fintrac-canafe/fintrac-canafe_e.pdf

[11] Financial Crimes Enforcement Network, "Press Release: Civil money penalties assessed against American Express Bank International and American Express Travel Related Services Company, Inc." – August 6, 2007. URL: http://www.fincen.gov/aebi_joint_release.pdf; Associated Press, "Feds say American Express is to pay $65 million for violating anti-money laundering law", *International Herald-Tribune*, August 6, 2007. URL: http://www.iht.com/articles/ap/2007/08/06/business/NA-FIN-US-Money-Laundering.php

[12] *Proceedings of the Standing Senate Committee on Banking, Trade and Commerce, The Review of the Proceeds of Crime (Money Laundering) and Terrorist Financing Act* – May 18, 2006 (Ottawa, Ontario), 2: p. 31-32. URL: http://www.parl.gc.ca/39/1/parlbus/commbus/senate/Com-e/bank-e/pdf/02issue.pdf

Concerns on the propriety of financial monitoring

We understand money laundering both rewards and supports criminal activities; we are aware that the financing of terrorist groups undermines Canadian and international security. While the Office of the Privacy Commissioner has limited knowledge of the world of money laundering or terrorist financing, we feel compelled to question the proportionality of the PCMLTFA and the scope of its invasiveness into the everyday lives of Canadians. One of the difficulties with the recent expansion of Canada's anti-money laundering/anti-terrorist financing (AML/ATF) regime is that it is a "one size fits all" approach. We recognize the need to ensure that Canada does not become a safe haven for money launderers; our concerns relate to the regime's ever-growing scope.

There are also fundamental differences in the way countries traditionally deal with threats to national security versus their responses to criminal activity. In recent years, harmonized international approaches to combating money laundering and terrorist financing have largely ignored the legal reality that different countries have different approaches to privacy and the protection of personal information. Many countries still have relatively weak or even non-existent privacy/data protection laws. Subsequently, data collected under one rationale can be exploited for other purposes; this is in sharp contrast to Canada's privacy regime, but potential over-use or misuse is still a concern.

In addition, we feel a clear and compelling case has still not been made for the expansion of Canada's anti-money laundering regime. While the Office has closely monitored the debate, we have never been privy to a clear estimate of the problem's size, nor do we know if the current regime is an effective deterrent. After reviewing recent committee appearances of officials from the Department of Finance, Justice, Public Safety and FINTRAC, precise figures on prosecutions or overall trends remain elusive.[13] Little evidence demonstrating the need for the expansion of monitoring was presented. Rather, officials stated the Act simply had to be updated to meet international commitments, especially in light of a 2006 Financial Action Task Force review grading Canadian efforts to tighten financial monitoring.[14]

As a result, the magnitude of both money laundering and terrorist financing in Canada is unclear. As the Office of the Auditor General stated in its 2003 report to Parliament, "there are no reliable estimates of either the extent or impact of money laundering in Canada ... estimates that are frequently used in Canada and internationally should be viewed with a degree of scepticism."[15] Without reliable data on the extent of this activity, subsequent analysis and debate has often been equally vague and hypothetical. This makes it very hard to ascertain whether the privacy impacts for Canadians tally at all reasonably with the scope of the problem or the cost of combating it.

Concerns raised by other Parliamentary reviews

---

[13] Ibid, 2: 13, 29-30, 38, 40-41, 49-52, 57, 62.

[14] Department of Finance, *Press Release and Backgrounder: Canada's New Government Toughens Anti-Money Laundering and Anti-Terrorist Financing Regime* (Ottawa, October 5, 2006). URL: http://www.fin.gc.ca/news06/06-055e.html

[15] Office of the Auditor General of Canada, *Report of the Auditor General to the House of Commons – Chapter Three: Canada's Strategy to Combat Money Laundering* (Ottawa, 2003), p. 8. URL: http://www.oag-bvg.gc.ca/domino/reports.nsf/html/20030403ce.html/$file/20030403ce.pdf

We were encouraged that the need for greater oversight over the operations of FINTRAC has been recognized. The Senate Banking Committee, for example, recommended periodic reviews be conducted by the Security and Intelligence Review Committee (SIRC) and it went on to recommend that SIRC should receive adequate resources to enable it to fulfill this broader mandate. The intelligence gathering activities of various federal organizations have grown vastly in resources, scope and personnel since 2001; governance and safeguards have not developed proportionately.

While some review activity has been strengthened, there is still need for holistic, integrated oversight. Recent amendments require the Office of the Privacy Commissioner to conduct a review every two years of FINTRAC measures to protect personal and to submit a report to Parliament.[16] However, given the nature of intelligence gathering and information sharing across government departments and agencies, focussing on the data protection practices within a single organization may miss the much larger picture.

In July 2007, the Government of Canada issued its response to the House of Commons review of *Canada's Anti-Terrorism Act* (ATA). The Government's response suggests financial monitoring may continue to broaden yet again. For example, there are strong indications lawyers should no longer be exempt from reporting, as the Government has rejected the House of Commons recommendation to disallow lawyers from the regime in order to safeguard solicitor-client privilege.[17]

Suggestions to the Commission

We are not alone in raising questions about the privacy implications of the AMLATF regime. Parliament gave the issue enough weight to amend the act as noted above, requiring our Office to conduct regular audits. The Commission of Inquiry into the Actions of Canadian Officials in Relation to Maher Arar also called for increased oversight of FINTRAC; so too did the Senate Committee during its five-year review of the Act. We would urge these recommendations be given consideration by this Inquiry.[18]

There should also be an increased role and additional resources for the SIRC to broadly oversee the national security activities of departments and agencies. To date these recommendations have not become policy, although in its July 2007 response, the Government indicated it will develop a process for national security review consistent with recommendations of the *Commission of Inquiry into the Actions of Canadian Officials in Relation to Maher Arar* and may enhance the role for Parliament in security oversight.[19] Given our concerns, we would reiterate to the current Inquiry the urgency and importance of this commitment.

---

[16] *Proceeds of Crime (Money Laundering) and Terrorist Financing Act*, section 72 (2). URL: http://laws.justice.gc.ca/en/ShowFullDoc/cs/P-24.501///en

[17] Government of Canada, *Response of the Government of Canada to the Final Report of the Standing Committee on Public Safety and National Security Subcommittee on the Review of the Anti-Terrorism Act – Rights, Limits, Security: A Comprehensive Review of the Anti-Terrorism Act and Related Issues* (Ottawa, 2007), p. 8. URL: http://cmte.parl.gc.ca/Content/HOC/committee/391/secu/govresponse/rp3066235/391_SECU_Rpt07_GR/391_SECU_Rpt07_GR-e.pdf

[18] 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*, p. 561-2. URL: http://www.ararcommission.ca/eng/EnglishReportDec122006.pdf

[19] Ibid, 25

Providing individuals with a right of access to their own personal information is one of the fundamental fair information principles that underlie the protections found in federal privacy legislation. Allowing individuals to see the information that government agencies or private sector organizations hold about them, or have disclosed to others, acts as an important check on the practices of organizations. Canada's anti-terrorist financing regime effectively removes these checks and balances and significantly weakens privacy protections provided by the two federal Acts (PIPEDA and the *Privacy Act*). While the Office of the Privacy Commissioner will audit FINTRAC on a regular basis, auditing the thousands of Canadian businesses that are sending information about their customers to FINTRAC, without their customers' knowledge is impossible. From a privacy perspective, it is critically important to *minimize* the scope of the regime.

We also urge the Commission to weigh the completeness and adequacy of the institutional framework (including the Privacy Act and Office of the Privacy Commissioner) to safeguard privacy rights in light of expanded monitoring for anti-terrorist financing. Accountability structures that can assess the regime's performance, openness and transparency are critical. As amended, the Act now requires the Office of the Privacy Commissioner of Canada to conduct a review every two years of measures taken by FINTRAC to protect information it receives or collects under this Act and submit a report to Parliament. As reported, the OPC will also conduct an audit of FINTRAC in 2007-08 pursuant to our authority under the *Privacy Act*. This audit would include review of operational case files, security assessments (both physical and IT), internal reports, Memorandum of Understanding with other organizations and so forth. Our Office will review several aspects of the Centre's operations with a particular emphasis on the amount and type of personal information collected and the safeguards used to protect it.

In closing, the Proceeds of Crime (Money Laundering) and Terrorist Financing Act is an inherently intrusive Act at odds with the protection of privacy. The Act treats everyone as a potential suspect, weakens existing privacy protections, and enlists a wide range of businesses and professionals in the fight against money laundering and terrorist financing by requiring them to monitor the activities of their customers and make judgments about their behaviour. A privacy sensitive regime requires transparency, openness and effective oversight. We would suggest the Commission urge FINTRAC to deepen internal controls proactively -for example, robust internal audit processes, de-identification and compartmentalization of data, layered security, forgoing transfer of financial data to countries with privacy regimes weaker than our own – all with the goal of ensuring that businesses do not over-report on their clients, that FINTRAC does not disclose personal information inappropriately and that the sensitive financial data of Canadians is well-protected.