



Homeland Security

The following document was received by the DHS Privacy Office on behalf of the DHS Data Privacy and Integrity Advisory Committee.

Trevor Shaw

Director General, Audit and Review Branch
Office of the Privacy Commissioner, Canada

Background Materials:

[Jennifer Stoddart's testimony on Anti-terrorism Act in Canada](#)

For more information please visit: www.dhs.gov/privacy or email the DHS Privacy Office: privacy@dhs.gov or the DHS Data Privacy and Integrity Advisory Committee: privacycommittee@dhs.gov.

Additional Contact Information:

Data Privacy and Integrity Advisory Committee
The Privacy Office
U.S. Department of Homeland Security
Washington, DC 20528
Telephone: 571-227-3813
Fax: 571-227-4171



Office of the
Privacy Commissioner
of Canada

Commissariat
à la protection de
la vie privée du Canada

Canada

Français	Contact Us	Help	Search	Canada Site
Home	What's New	About Us	FAQs	Site Map

Resource Centre



Anti-terrorism Act

Subcommittee on Public Safety Act and National Security

June 1, 2005
Ottawa, Ontario

Opening Statement by Jennifer Stoddart
Privacy Commissioner of Canada

(CHECK AGAINST DELIVERY)

Mr. Chairman, members of the Subcommittee.

Thank you for inviting me to appear today to discuss the *Anti-terrorism Act*.

My remarks today will focus primarily on the lack of facts and evidence to suggest that the measures provided for by the *Anti-terrorism Act* are necessary. We urge the Subcommittee to critically assess the issue of proportionality and to consider a number of our proposed practical recommendations to address the cumulative impact of anti-terrorism measures on the privacy rights of Canadians.

Anti-terrorism and the right of privacy

No one denies the reality of the threat that the Act was intended to address. We must ask ourselves, however, whether what the Act gains us in security justifies the sacrifice of privacy and other rights. Regrettably, there appears to exist no empirical evidence shared with Canadians to suggest that the measures provided for by the *Anti-terrorism Act* are necessary. This is one of the paradoxes of the present exercise and it prompts my first comment to you that this Act, should be subject in its entirety to a recurring sunset clause.

Specifically, the impacts of the Act can be grouped into three broad themes.

- First, the surveillance powers of security and intelligence and law enforcement agencies have been overly broadened.
- Second, constraints on the use of those same surveillance powers have been unduly weakened.
- Third, government accountability and transparency have been significantly reduced.

Broadened Surveillance Powers

Since 9/11, the Canadian government has introduced a series of measures to broaden its surveillance powers over the citizens and residents of Canada.

The *Anti-terrorism Act* has set the tone for creating a broader net for surveillance of organizations and individuals. It was accompanied by changes to the *Aeronautics Act*, the *Public Safety Act* and *PIPEDA*. It will soon be followed by "lawful access" proposals. Much of the personal information

gathered is highly sensitive and part of integrated information systems that could impact the lives of Canadians if the information were misused, distorted or misinterpreted.

However, public opinion trends, including a recent poll by my office, suggests that Canadians are increasingly aware of informational privacy issues and expect a reasonable and balanced approach to a national strategy to combat terrorism. The poll shows there is strong support by the public for greater accountability, transparency and oversight of agencies involved in national security.

There is a real risk that as the logic of anti-terrorism permeates all spheres of law enforcement and public safety, large-scale systems of surveillance will increasingly erode privacy rights in Canada, without a critical assessment of where it is appropriate to draw the line. ID cards, uncritical use of new technology, such as RFIDs, increased data mining and integrated law enforcement systems are other looming threats to privacy.

Reduced Constraints on Surveillance

At the same time that the surveillance powers of the state have been strengthened by the *Anti-terrorism Act*, constraints on those powers have been weakened.

Law enforcement and national security agencies are no longer required, in anti-terrorism investigations, to consider other investigative methods prior to applying for judicial authorization for electronic surveillance.

The executive branch of government may displace the role of the judiciary in issuing security certificates and authorizing interception of communications; and the judicial standard of "reasonable grounds to believe" has been lowered to one of "reasonable grounds to suspect."

A number of the legislative amendments enacted under the *Anti-terrorism Act* have had the effect of weakening independent oversight of the surveillance activities of law enforcement and security and intelligence organizations.

Independent oversight is one of the pillars of democratic freedom. The question, "Who watches the watchers?" is best answered by ensuring oversight of the surveillance powers of the state by the judiciary and other independent agents. Parliament and Canadians need to question the measures in the *Anti-terrorism Act* that reduce oversight. Independent review and integrated monitoring, including that of oversight agencies themselves should be the rule, not the exception.

Decreased Government Transparency

Amendments brought about by the *Anti-terrorism Act* have also added to the secrecy surrounding legal proceedings, contrary to the fundamental principles that court hearings should be conducted openly and that individuals should be entitled to know the charges against them and the evidence relevant to the charges.

Among the most significant changes affecting transparency and access of individuals to their own personal information are the amendments to section 38 of the *Canada Evidence Act*, the section that addresses the judicial balancing of interests between the public interest in disclosure and the interest of the state in national security and maintaining foreign confidences.

As amended by the *Anti-terrorism Act*, section 38 of the *Canada Evidence Act* provides a broad statutory gag order that prohibits not only the disclosure of the information itself, but also the mere fact that section 38 proceedings have been engaged.

These restrictions on disclosure are, in many cases, overly broad.

The *Anti-terrorism Act* further amends section 38 procedures by permitting the Attorney General to override a Federal Court order that the information should be disclosed.

This extraordinary power is unnecessary in view of the judicial rigor that already exists under the *Canada Evidence Act*, which appropriately allows a judge to determine the balance of the competing interests between disclosure and national security.

Recommendations

My Office has tabled with the Subcommittee a position paper outlining 18 practical recommendations aimed at improving the provisions and operation of the *Anti-terrorism Act*.

Our recommendations aim to contain surveillance, as well as increase oversight and promote transparency. We also ask that the Subcommittee consider some general recommendations aimed at improving the privacy protection regime of the federal government's national security framework.

My first recommendation of the paper stipulates that the Government of Canada should conduct an empirical assessment of the effectiveness of the extraordinary powers granted to law enforcement and national security agencies under the *Anti-terrorism Act*, and the proportionality of the loss of established rights.

This examination should include an exploration of alternative models for achieving national security objectives without unnecessarily encroaching on informational privacy.

As I indicated a moment ago, there exists an apparent lack of empirical assessment by the government of the effectiveness of the extraordinary powers that the *Anti-terrorism Act* gives law enforcement and national security agencies. This assessment is the necessary precondition of a proper analysis of proportionality.

I have also formulated seven recommendations in the paper that address the need for contained surveillance and increased oversight. The suggestions include increased judicial oversight over the activities of law enforcement agencies.

The paper includes four recommendations on the need for transparency and openness of Section 38 procedures under the *Canada Evidence Act*. We believe these recommendations will strike the right balance between disclosure and national security interests.

I have also created a recommendation for a security-cleared special advocate position to carry out the function of both challenging arguments that information should not be disclosed to the affected party, and in challenging information that cannot be disclosed before the judge. Our Office would be willing to offer its policy expertise and experience in applying privacy legislation to assist in the development of special advocates.

Finally I have made five general recommendations of importance that deal with the need for a continuing review of the Act and a proposal that the Government articulate the operating principles of a privacy management framework for national security, including the development of an internal privacy audit capacity, privacy leadership responsibilities incorporated in the performance agreement of senior executives, privacy protection performance indicators, and a strengthened role for Access to Information and Privacy coordinators.

As I indicated earlier, Canadians are very concerned about the transfer of their personal information to foreign government agencies. In response to these concerns, my office has launched a major audit of the Canada Border Service Agency, which as you know, is an integral part of the PSEP portfolio.

The objective of this audit is to assess the extent to which the CBSA is adequately controlling and protecting the flow of Canadians' personal information to foreign governments or institutions thereof. The premise of this audit is that national security objectives and sound personal information management practices are mutually dependent.

Underlying this hypothesis is the belief that strong controls over the handling of personal information, will limit privacy risks such as improper uses or disclosures, which will also support a robust National Security framework.

Collection, use and disclosure of personal information must be limited to that which is necessary and permissible by law and should be circumscribed by multiple layers of privacy and security protections during its entire life-cycle to prevent and mitigate risks that may impact equally on personal privacy as well as on national security objectives.

The audit will examine several key operational systems used to process personal information collected, processed and shared by CBSA with US counterparts. The audit will also assess the overall robustness of CBSA's privacy management regime as well as how it reports on its privacy management responsibilities to Parliament and the public.

The elements of a privacy management framework discussed earlier will be familiar to the Government. Indeed, I recently wrote to the President of the Treasury Board to suggest a number of measures to strengthen the Government's privacy management regime. These range from a thorough review of outsourcing and off-shoring of personal information and the development of contractual clauses to mitigate against privacy risks, to strengthening the reporting requirements to Parliament under the *Privacy Act*.

Since accepting the invitation to meet with your Subcommittee to review the *Anti-terrorism Act*, we have received a response from Minister Alcock to our suggestions to reinforce the Privacy Management Framework of the federal government.

On the review of outsourcing implications resulting from transborder flow of information and the *USA PATRIOT Act*, the Minister outlined the government's multi-pronged approach which includes carrying out a government-wide assessment of potential risks to the personal information of Canadians, the development of contractual clauses to build protection throughout the contracting process and providing clear communications to Deputy Heads and the Canadian public on a federal action plan and strategy to deal with transborder flows.

The Minister states that the results of the comprehensive review and the action plan would be publicly released this summer. On the development of contractual clauses to mitigate against potential privacy risks resulting from outsourcing, the Minister states that these are now being reviewed by legal experts and that my Office would have an opportunity to review and comment on them.

On data mining or data aggregation, the minister states that there is a need to scope the nature and magnitude of the issue.

On data matching, the minister informs us that amendments are being brought to the Data Matching Policy which will include a more encompassing definition of data match to include front end data verification, data mining and other back-end data matches.

On Annual reporting requirements, under section 72 of the *Privacy Act*, the Treasury Board Secretariat just recently released new guidance to Deputy Heads which asks them to provide a more comprehensive reporting of their personal information management including section 8 (2) disclosures, data matching and Privacy Impact Assessments. The Minister also suggests that a model reporting template for federal institutions be developed. In light of our discussion of the ATA, I would further suggest that this new reporting template be tested on PSEP agencies in this fiscal year.

The minister's response indicates that the federal government is taking its responsibilities to reinforce the privacy management framework seriously, although we have been flagging the need for a cogent response to the *USA PATRIOT Act* since February 2004.

Concluding Remarks

In closing, let me state simply that the *Anti-terrorism Act* — as well as other recent government initiatives aimed at combating terrorism — reflects a fundamental shift in the balance between national security, law enforcement and informational privacy, with a associated loss of privacy and due process protections for individuals.

Over-broad state powers in the name of national security may in fact imperil the self-identity of

democratic nation states. It is imperative that the means and measures adopted to combat security threats do not end up abrogating the very freedoms that define and give substance to the democracy that we claim to be defending.

Contrary to what is sometimes thought, security and the protection of informational privacy need not be seen as a trade-off, where one is sacrificed in the interest of the other. Both can be achieved with well-designed law, prudent policy, and effective but not excessive oversight.

I urge the Subcommittee to carefully consider our remarks and recommendations, which are intended to contribute to the achievement of this goal.

Thank you.

Summary of Recommendations on the *Anti-terrorism Act* Presented to the Subcommittee on Public Safety Act and National Security

June 1, 2005

Recommendation 1

The Government of Canada should conduct an empirical assessment of the effectiveness of the extraordinary powers granted to law enforcement and national security agencies under the *Anti-terrorism Act*, and the proportionality of the loss of established rights. The examination should include an exploration of alternative models for achieving national security objectives without unnecessarily encroaching on informational privacy.

Recommendation 2

The ordinary requirement that a judge be convinced that other methods of investigation have been tried or would fail should be applied to electronic surveillance for terrorism offences under the *Criminal Code*.

Recommendation 3

The *Criminal Code*'s ordinary time limits for such warrants — 60 days authorization and up to one year for notification — should be required, and the exceptions in the *Anti-terrorism Act* for warrants up to a year and up to three years without authorization should be repealed.

Recommendation 4

The *Anti-terrorism Act*'s amendments to the *National Defence Act* to allow the interception of private conversations that may involve people in Canada should be amended to require prior judicial authorization.

Recommendation 5

The requirement in section 273.65(2)(d) of the *National Defence Act* 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.

Recommendation 6

Section 273.65(4)(d) of the *National Defence Act*, which permits CSE to collect information essential to protecting the government's computer systems, should be amended to place limitations on what information CSE can *obtain*.

Recommendation 7

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 in fact 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*.

Recommendation 8

Parliament should undertake a systematic review of the overall mechanism for oversight of national security activities, taking into account the existing bodies and identifying areas where these bodies overlap, but more importantly, identifying areas where there are gaps in coverage.

Recommendation 9

The mandatory *in camera* proceedings and the mandatory ban on even revealing that a s.38 proceeding is taking place found in ss.38.02 and 38.11 should be repealed, following the principles in *Ruby v. Canada* and the comments by Chief Justice Lutfy in the *Ottawa Citizen Group* case. A more proportionate alternative is to allow the judge to hold proceedings *in camera* when necessary to protect national security.

Recommendation 10

Section 38.13 should be repealed on the basis that it is superfluous to empower the executive to trump an adjudicative order for disclosure. Section 38.06 already allows courts to balance the conflicting interests in disclosure and national security and impose conditions on the release of information in a manner that reconciles these two important concerns; it has been interpreted by the courts in a way that makes generous allowance for the state's interests in national security, national defence and international relations.

Recommendation 11

Should s.38.13 certificates be retained, they should be subject to the same reporting and sunset requirements as the use of investigative hearings and preventive arrests, because they constitute extraordinary interventions by the executive into the adjudicative process. A section 38.13 certificate should also not last for 15 years but for 5 years, perhaps subject to renewal.

Recommendation 12

A judicial balancing of competing disclosure and security interests as available under s.38.06 should also be available under s.38.131, which provides for review by one judge of the Federal Court of Appeal of a s.38.13 certificate issued by the Attorney General. Thought should also be given to allowing appeals from the judicial review of the s.38.13 certificate, or of allowing the review to be conducted by three as opposed to one judge of the Federal Court of Appeal, so as to encourage greater checks and balances and the possibility for the expression of dissent.

Recommendation 13

I recommend that the Subcommittee give consideration to the creation of a security-cleared special advocate position, to test Government claims that information should not be disclosed because of concerns about national security. This would ensure that a judge hears an advocate for the greatest possible disclosure possible before making a decision. The special advocate could also

examine any evidence that the judge decides cannot be disclosed to the affected person and, where appropriate, challenge the government's reliance on such secret evidence.

Recommendation 14

The *Anti-terrorism Act*, along with the *Public Safety Act*, should be considered extraordinary legislation. As such, they should be subject to periodic Parliamentary review to assess their continued relevance, and to keep them in the public eye.

Recommendation 15

The Government should articulate the operating principles of a *privacy management framework*, including the development of internal privacy audit capacity, privacy leadership responsibilities incorporated in the performance agreement of senior executives, privacy protection performance indicators, and a strengthened role for Access to Information and Privacy coordinators.

Recommendation 16

Departments and agencies with an anti-terrorism role under the *Anti-terrorism Act* should be required to report to Parliament on a periodic basis, perhaps at the same time as the legislative review, with a general description of their anti-terrorism programs, and accounting of how effective these measures have been for detecting, stopping or deterring terrorist acts.

Recommendation 17

The Government should establish a National Security Committee of Parliamentarians to oversee the security and intelligence apparatus in Canada. Such a committee would review the policies, resources and legislation supporting Canada's national security system, assess their effectiveness, and identify required improvements. The Committee should be supported by security cleared staff and have access to all information, including classified information, required to carry out its mandate.

Recommendation 18

The Government of Canada should, in the context of the new national security environment, examine the adequacy of legislation that governs personal information collected, processed and shared by the Canadian government. This means a thoroughgoing reconsideration of the *Privacy Act*, of course, something that has been seriously overdue since before 9/11. The Government of Canada and Parliament should also assess the completeness and adequacy of the institutional framework (including the Office of the Privacy Commissioner) to safeguard privacy rights, and the powers and authorities of oversight bodies, including their capabilities and resources.

Date published: 2005-06-03
Date modified: 2005-06-03



[Important Notices](#)