The Privacy Commissioner of Canada

Commissaire à la protection de la vie privée du Canada

Annual Report to Parliament 2001-2002

The Privacy Commissioner of Canada

Commissaire à la protection de la vie privée du Canada

Annual Report to Parliament 2001-2002

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

(613) 995-8210, 1-800-282-1376
Fax (613) 947-6850
TDD (613) 992-9190

Cat. No. IP30-1/2002
ISBN 0-662-66668-2

This publication is also available on our Web site at **www.privcom.gc.ca**

Office of the Privacy Commissioner of Canada

112 Kent Street
Ottawa, Ontario
K1A 1H3
Tel.: (613) 995-8210
Fax: (613) 947-6850
1-800-282-1376
www.privcom.gc.ca

Commissariat à la protection de la vie privée du Canada

112, rue Kent
Ottawa (Ontario)
K1A 1H3
Tél. : (613) 995-8210
Télec. : (613) 947-6850
1-800-282-1376
www.privcom.gc.ca

January 2003

The Honourable Daniel Hays
The Speaker
The Senate of Canada

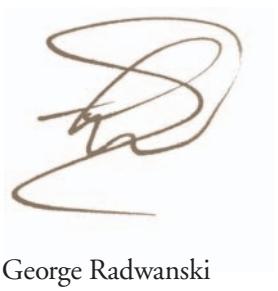
Dear Mr. Hays:

I have the honour to submit to Parliament my Annual Report which covers the period from April 1, 2001 to March 31, 2002 for the *Privacy Act* and from December 1 to 31, 2001 for the *Personal Information Protection and Electronic Documents Act*.

I had originally intended this report to be released last spring. The year 2002 was a tumultuous one for privacy, however, and I was reluctant to report to Parliament while major issues, particularly issues involving the crucial balance between privacy and security in the aftermath of September 11, remained unresolved. In keeping with my mandate as an ombudsman for the privacy rights of Canadians, I continued to seek resolutions of these issues with ministers and senior public servants. To date, despite repeatedly extending my deadlines, I have not been successful. Obviously, I cannot ask Parliament to wait indefinitely, and must submit my report despite this inconclusive and unsatisfactory state of affairs.

I will report on the experience with the second year of the *Personal Information Protection and Electronic Documents Act* in my next annual report.

Yours sincerely,



George Radwanski
Privacy Commissioner of Canada

Office of the Privacy Commissioner of Canada

112 Kent Street
Ottawa, Ontario
K1A 1H3
Tel.: (613) 995-8210
Fax: (613) 947-6850
1-800-282-1376
www.privcom.gc.ca

Commissariat à la protection de la vie privée du Canada

112, rue Kent
Ottawa (Ontario)
K1A 1H3
Tél. : (613) 995-8210
Télec. : (613) 947-6850
1-800-282-1376
www.privcom.gc.ca

January 2003

The Honourable Peter Milliken
The Speaker
The House of Commons

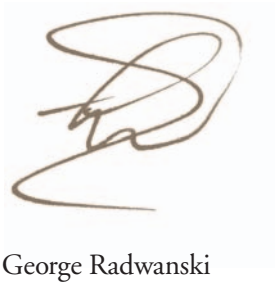
Dear Mr. Milliken:

I have the honour to submit to Parliament my Annual Report which covers the period from April 1, 2001 to March 31, 2002 for the *Privacy Act* and from December 1 to 31, 2001 for the *Personal Information Protection and Electronic Documents Act*.

I had originally intended this report to be released last spring. The year 2002 was a tumultuous one for privacy, however, and I was reluctant to report to Parliament while major issues, particularly issues involving the crucial balance between privacy and security in the aftermath of September 11, remained unresolved. In keeping with my mandate as an ombudsman for the privacy rights of Canadians, I continued to seek resolutions of these issues with ministers and senior public servants. To date, despite repeatedly extending my deadlines, I have not been successful. Obviously, I cannot ask Parliament to wait indefinitely, and must submit my report despite this inconclusive and unsatisfactory state of affairs.

I will report on the experience with the second year of the *Personal Information Protection and Electronic Documents Act* in my next annual report.

Yours sincerely,



George Radwanski
Privacy Commissioner of Canada

Table of Contents

Commissioner's Overview

It is my duty, in this Annual Report, to present a solemn and urgent warning to every Member of Parliament and Senator, and indeed to every Canadian:

The fundamental human right of privacy in Canada is under assault as never before. Unless the Government of Canada is quickly dissuaded from its present course by Parliamentary action and public insistence, we are on a path that may well lead to the permanent loss not only of privacy rights that we take for granted but also of important elements of freedom as we now know it.

We face this risk because of the implications, both individual and cumulative, of a series of initiatives that the Government has mounted or is actively moving toward. These initiatives are set against the backdrop of September 11, and anti-terrorism is their purported rationale. But the aspects that present the greatest threat to privacy either have nothing at all to do with anti-terrorism, or they present no credible promise of effectively enhancing security.

The Government is, quite simply, using September 11 as an excuse for new collections and uses of personal information about all of us Canadians that cannot be justified by the requirements of anti-terrorism and that, indeed, have no place in a free and democratic society.

As of the date this Report went to press, January 17, the Government has shown no willingness to modify these initiatives in response to privacy concerns. Whether the Government's awareness of the imminence of this Report will have brought about any change by the time the Report is tabled, I cannot foresee.

I wish to emphasize at the outset that I have never once raised privacy objections against a single actual anti-terrorist security measure. Indeed, I have stated repeatedly ever since September 11 that I would never seek as Privacy Commissioner to stand in the way

George Radwanski
Privacy Commissioner of Canada

of any measures that might be legitimately necessary to enhance security against terrorism, even if they involved some new intrusion or limitation on privacy.

I have objected only to the extension of purported anti-terrorism measures to additional purposes completely unrelated to anti-terrorism, or to intrusions on privacy whose relevance or necessity with regard to anti-terrorism has not been in any way demonstrated. And still the Government is turning a resolutely deaf ear.

Specifically, I am referring to: the Canada Customs and Revenue Agency's new "Big Brother" passenger database; the provisions of section 4.82 of Bill C-17; dramatically enhanced state powers to monitor our communications, as set out in the "Lawful Access" consultation paper; a national ID card with biometric identifiers, as advanced by Citizenship and Immigration Minister Denis Coderre; and the Government's support of precedent-setting video surveillance of public streets by the RCMP.

These initiatives are all cause for deep concern because of the intrusions on privacy that they directly entail. But they are even more disturbing because of the thresholds they cross and the doors they open. Each of these measures establishes a devastatingly dangerous new principle of acceptable privacy invasion.

The CCRA's database introduces the creation of personal information dossiers on all law-abiding citizens for a wide variety of investigative purposes. Section 4.82 of Bill C-17 requires, for the first time, de facto mandatory self-identification to the police for general law enforcement. The "Lawful Access" paper advocates the widespread monitoring of our communications activities and reading habits.

A national ID card would remove our right to anonymity in our day-to-day lives. The RCMP's video surveillance constitutes systematic observation of citizens by the police as we go about our law-abiding business on public streets.

These are not abstract or theoretical concerns. If these measures are allowed to go forward and the privacy-invasive principles they represent are accepted, there is a very real prospect that before long our lives here in Canada will look like this:

- All our travels outside Canada will be systematically recorded, tracked and analyzed for signs of anything that the Government might find suspicious or undesirable. "Big Brother" dossiers of personal information about every law-abiding Canadian – initially travel information, but eventually supplemented by who knows what else – will be kept by the federal Government and will be available to virtually every federal department and agency, just in case they are ever handy to use against us.

If the Government's current initiatives are allowed to go forward, there is a very real risk that privacy as we know it will soon become a distant, irretrievable memory.

- Any time we travel within Canada, we will have to identify ourselves to police so that their computers can check whether we are wanted for anything or are otherwise of interest to the state.
- Police and security will be able to access records of every e-mail we send and every cellular phone call we make. Information on what we read on the Internet, every Web site and page we visit, will likewise be readily available to government authorities.
- We will all be fingerprinted or retina-scanned by the Government. This biometric information will be on compulsory national ID cards that will open the way to being stopped in the streets by police and required to identify ourselves on demand.
- Our movements through the public streets will be relentlessly observed through proliferating police video surveillance cameras. Eventually, these cameras will likely be linked to biometric face-recognition technologies that will match our on-screen images to file photos – from such sources as drivers' licences, passports or ID cards – and enable the police to identify us by name and address as we go about our law-abiding business in the streets.

I am well aware that these scenarios are likely to sound, to most people, like alarmist exaggeration. Certainly, the society I am describing bears no relation to the Canada we know. But anyone who is inclined to dismiss the risks out of hand should pause first to consider that the privacy-invasive measures already being implemented or developed right now would have been considered unthinkable in our country just a short year ago.

I am not predicting that all this will necessarily happen. But I am warning with all the intensity at my disposal that, in each instance, once the principle has been accepted and the precedent has been established, further intrusions on privacy are only a matter of degree. That makes them virtually inevitable.

The place to stop unjustified intrusions on a fundamental human right such as privacy is right at the outset, at the very first attempt to enter where the state has no business treading. Otherwise, the terrain will have been conceded, and the battle lost.

Consequently, if the Government's current initiatives are allowed to go forward, there is a very real risk that privacy as we know it will soon become a distant, irretrievable memory.

The situation is made all the more worrisome by the fact that the Government is doing all this in blatant, open and repeated disregard of the concerns that it is my duty to express as the Officer of Parliament mandated to oversee and defend the privacy rights of all Canadians.

This disregard threatens the privacy rights of Canadians not only directly through the intrusive measures in question, but also

indirectly by undermining the whole edifice of privacy protection that has been in place in this country for nearly two decades.

Regrettably, this Government has lost its moral compass with regard to the fundamental human right of privacy.

It appears to have become convinced that privacy must be sacrificed bit by bit, day by day, in pursuit of greater goods: reassuring a public frightened by the outrages of September 11; mollifying an insistent U.S. government; meeting the wishes of police, security forces and other Government institutions that have recognized the aftermath of September 11 as an opportunity to expand their powers.

As well, the Government has become inappropriately willing to brush aside all criticism of its assault on privacy rights, apparently regarding such criticism as simply a cost of doing business. This criticism has come not only from me in the exercise of my mandate from Parliament to oversee and defend the privacy rights of Canadians, but also from a great many others who have publicly endorsed my concerns. These include seven provincial and territorial Information and Privacy Commissioners from across Canada, the Canadian Civil Liberties Association, the B.C. Civil Liberties Association, the B.C. Freedom of Information and Privacy Association, the *Ligue des droits et libertés*, Electronic Frontier Canada, the Commonwealth Centre for e-Governance, the Public Interest Advocacy Centre, and the Manitoba Association of Rights and Liberties.

In the nearly 20-year history of privacy protection since the position of Privacy Commissioner was created under the *Privacy Act* in 1983, a convention has been established that when the Privacy Commissioner points out that a practice or an initiative is inconsistent with privacy rights, the Government pays heed.

That's the way the system is supposed to work. I am an ombudsman, mandated by Parliament, whose role with regard to the federal Government is normally carried out primarily through persuasion and co-operative discussion behind the scenes. Like my predecessors, that is the way I have sought to operate since my appointment. I have recommended to ministers and senior Government officials specific solutions to enable them to achieve their legitimate policy objectives in ways that are more respectful of privacy rights. This has produced many successful outcomes which, by the very nature of the process, do not come publicly to light.

But in its approach to the aftermath of September 11, the Government has increasingly been turning its back on the cooperative nature of the federal privacy protection system by flatly refusing to pay attention. In each of the instances where I have been obliged to publicly criticize the Government for failing to respect the privacy rights of Canadians,

Governmental disregard for crucially important privacy rights is moving beyond isolated instances and becoming systematic. This puts a fundamental right of every Canadian profoundly at risk.

it was only after I had first made every effort to persuade the minister responsible with carefully reasoned arguments and had my expressions of concern ignored or brushed aside.

Now I am informing Parliament that there is every appearance that governmental disregard for crucially important privacy rights is moving beyond isolated instances and becoming systematic. This puts a fundamental right of every Canadian profoundly at risk. It is a trend that urgently needs to be reversed.

If the Government can, with impunity and without provoking the strongest response from Parliament, simply brush aside the Privacy Commissioner's warnings and do as it pleases, then privacy protection in this country will be progressively weakened, and worse and worse intrusions will be inevitable.

In the months immediately following September 11, I was in fact quite optimistic that, with regard to privacy, the Government was on the whole being balanced and thoughtful in its response. But now the floodgates appear to have burst.

Now "September 11" is invoked as a kind of magic incantation to stifle debate, disparage critical analysis and persuade us that we live in a suddenly new world where the old rules cannot apply.

If Parliament and the public at large have been slow to react, it is probably because for most people, most of the time, privacy is a pretty abstract concept. Like our health, it's something we tend not to think about until we lose it – and then discover that our lives have been very unpleasantly, and perhaps irretrievably, altered.

But though we tend to take it for granted, privacy – the right to control access to ourselves and to personal information about us – is at the very core of our lives. It is a fundamental human right precisely because it is an innate human need, an essential condition of our freedom, our dignity and our sense of well-being.

If someone intrudes on our privacy – by peering into our home, going through the personal things in our office desk, reading over our shoulder on a bus or airplane, or eavesdropping on our conversation – we feel uncomfortable, even violated.

Imagine, then, how we will feel if it becomes routine for bureaucrats, police officers and other agents of the state to paw through all the details of our lives: where and when we travel, and with whom; who are the friends and acquaintances with whom we have telephone conversations or e-mail correspondence; what we are interested in reading or researching; where we like to go and what we like to do.

"The right not to be known against our will – indeed, the right to be anonymous except when we choose to identify ourselves – is at the very core of human dignity, autonomy and freedom.

A popular response is: "If you have nothing to hide, you have nothing to fear."

By that reasoning, of course, we shouldn't mind if the police were free to come into our homes at any time just to look around, if all our telephone conversations were monitored, if all our mail were read, if all the protections developed over centuries were swept away. It's only a difference of degree from the intrusions already being implemented or considered.

The truth is that we *all* do have something to hide, not because it's criminal or even shameful, but simply because it's private. We carefully calibrate what we reveal about ourselves to others. Most of us are only willing to have a few things known about us by a stranger, more by an acquaintance, and the most by a very close friend or a romantic partner. The right not to be known against our will – indeed, the right to be anonymous except when we choose to identify ourselves – is at the very core of human dignity, autonomy and freedom.

If we allow the state to sweep away the normal walls of privacy that protect the details of our lives, we will consign ourselves psychologically to living in a fishbowl. Even if we suffered no other specific harm as a result, that alone would profoundly change how we feel. Anyone who has lived in a totalitarian society can attest that what often felt most oppressive was precisely the lack of privacy.

But there also will be tangible, specific harm.

The more information government compiles about us, the more of it will be wrong. That's simply a fact of life.

Several years ago, after the existence of Human Resources Development Canada's "Longitudinal Labour Force File" was brought to light by my predecessor, many people demanded to see the information that had been held about them. They were astonished by the number of factual errors. That was only a research database, so its inaccuracies probably would have remained relatively benign even if it had not been dismantled.

But if our privacy becomes ever more systematically invaded by the state for purposes of assessing our behavior and making judgments about us, wrong information and misinterpretations will have potential consequences.

If information that is actually about someone else is wrongly applied to us, if wrong facts make it appear that we've done things we haven't, if perfectly innocent behavior is misinterpreted as suspicious because authorities don't know our reasons or our circumstances, we will be at risk of finding ourselves in trouble in a society where everyone is regarded as a suspect. By the time we clear our names and establish our innocence, we may have suffered irreparable financial or social harm.

> If we have to live our lives weighing every action, every communication, every human contact, wondering what agents of the state might find out about it, analyze it, judge it, possibly misconstrue it, and somehow use it to our detriment, we are not truly free.

Worse yet, we may never know what negative assumptions or judgments have been made about us in state files. Under exemptions to the general right of access under the *Privacy Act*, Canadians do not have the right to see the personal information that the Government holds about them if it pertains to national security or an ongoing investigation.

Decisions detrimental to us may be made on the basis of wrong facts, incomplete or out-of-context information or incorrect assumptions, without our ever having the chance to find out about it, let alone to set the record straight.

That possibility alone will, over time, make us increasingly think twice about what we do, where we go, with whom we associate, because we will learn to be concerned about how it might look to the ubiquitous watchers of the state.

- You stopped briefly in Thailand during a business trip, and liked it so much that you're thinking of going back on a vacation. But might repeat travel to Thailand get you flagged by the Government's analysts as a possible pedophile going there for the child sex trade? Could you find yourself detained for questioning every time you travel? Might you be denied security clearances, or refused entry into the United States?
- You're passing time browsing on the Internet and you're idly curious about what kind of propaganda in favour of al-Qaeda various extremists might be putting out. But could visiting such Web sites get you identified as a potential terrorist yourself and bring CSIS or RCMP officers knocking on your door?
- You're stopped on the street by a stranger asking for directions. But if by then proliferating street video surveillance cameras are linked to biometric face-recognition technology, what if the system immediately identifies the stranger as a known or suspected terrorist? If the police officer then calls up your name and address by matching your onscreen image to your driver's license or passport photo, will you go into security files yourself as a suspicious individual who had a street meeting with a terrorism suspect? Would you do better to keep walking whenever any stranger tries to talk to you?

The bottom line is this: If we have to live our lives weighing every action, every communication, every human contact, wondering what agents of the state might find out about it, analyze it, judge it, possibly misconstrue it, and somehow use it to our detriment, we are not truly free.

That sort of life is characteristic of totalitarian countries, not a free and open society like Canada. But that is where we are inexorably headed, if the Government's current initiatives are allowed to proceed.

Let me very briefly address the specifics of these objectionable initiatives, before suggesting some broader considerations that I believe should guide us in the post-September 11 environment.

The CCRA "Big Brother" database

In late 2001, under amendments to the *Customs Act*, Customs officers of the CCRA were given access to Advance Passenger Information (API) and the far more detailed Passenger Name Record (PNR) about every passenger flying into Canada from a foreign destination. The stated purpose of this was to facilitate identifying individuals who merit more careful questioning or examination on arrival.

When this legislation was before Parliament, I sought and received a formal written undertaking from the CCRA that, except in those relatively few instances where this API/PNR information did in fact cause an individual to be identified for secondary screening, it would all be destroyed within 24 hours. On the basis of this unequivocal undertaking that there would be no widespread retention, I did not express any privacy objection to providing Customs with this passenger information and did not find it necessary to appear before the House and Senate committees that studied the proposed amendments.

Last summer, the CCRA informed me that, contrary to its past undertaking, it has decided to keep all API/PNR information about Canadian travellers for six years in a massive new database.

All this personal information – more than 30 data elements including every destination to which we travel, who we travel with, how we pay for the tickets (sometimes including credit card numbers), what contact numbers we provide, even any dietary preferences or health-related requirements we communicate to the airline – will be available for an almost limitless range of governmental purposes under the broad information-sharing provisions of the *Customs Act*.

Those purposes, by the Government's own account, include everything from routine income tax investigations to trying to flag Canadians as potential pedophiles or money launderers solely on the basis of their travel patterns.

This is unprecedented. The Government of Canada has absolutely no business creating a massive database of personal information about all law-abiding Canadians that is collected without our consent from third parties, not to provide us with any service but simply to have it available to use against us if it ever becomes expedient to do so. Compiling

> It is difficult to imagine a more flagrant disregard for the rights of Canadians. This database is legally wrong and morally wrong.

dossiers on the private activities of all law-abiding citizens is the sort of thing the Stasi secret police used to do in the former East Germany. It has no place in a free and democratic society.

The CCRA's purported reason for creating this database is "forensic": In the event that there is a terrorist attack and some of the perpetrators are known, it wants to be able to use this database in search of any accomplices or associates. The CCRA has absolutely no mandate under the *Customs Act* to gather information for this sort of after-the-fact anti-terrorist forensic investigation.

But I have repeatedly asked Revenue Minister Elinor Caplan at least to limit the uses of this database to this exceptional anti-terrorist purpose, by strictly exempting it from the normal information-sharing provisions of the *Customs Act*. She flatly refuses.

The creation of this CCRA database lacks Parliamentary authority. It contravenes the *Privacy Act*. And there is overwhelming reason to believe that it is contrary to the *Canadian Charter of Rights and Freedoms*.

I have provided to Minister Caplan and to the Government, and made public, three separate independent legal opinions from the most eminent of authorities: retired Supreme Court Justice Gérard V. La Forest, who wrote many of the Court's most important decisions on privacy rights; former federal Deputy Minister of Justice Roger Tassé, who played a key role in drafting the *Canadian Charter of Rights and Freedoms*; and Hon. Marc Lalonde, who was a highly respected Minister of Justice in the Trudeau cabinet. All three state that this database clearly appears to be in violation of the *Charter*. This unprecedented trilogy of opinions has met with apparent indifference.

It is difficult to imagine a more flagrant disregard for the rights of Canadians. This database is legally wrong and morally wrong. If the Government can get away with systematically logging and analyzing all the foreign travel activities of every law-abiding citizen, then no other private activity will long be safe from being included in the same personal dossiers – our shopping, our banking, our communications, our movements within the country. The "Big Brother" society will be irrevocably upon us.

Bill C-17, the *Public Safety Act, 2002*

In the *Public Safety Act, 2002*, Bill C-17, the Government has reintroduced, with only minimal changes, a provision from the previous Bill C-55 that would give the RCMP and CSIS unrestricted access to the personal information held by airlines about all Canadian air travellers on domestic as well as international flights.

I have raised no objection to the primary purpose of this provision, section 4.82, which is to enable the RCMP and CSIS to use this passenger information for anti-terrorist

"If the police were able to carry out their regular *Criminal Code* law enforcement duties without this new power before September 11, they should likewise be able to do so now.

"transportation security" and "national security" screening. But my concern is that the RCMP would also be expressly empowered to use this information to seek out persons wanted on warrants for *Criminal Code* offences that have nothing to do with terrorism, transportation security or national security.

The implications of this are extraordinarily far-reaching. In Canada, it is well established that we are not required to identify ourselves to police unless we are being arrested or we are carrying out a licensed activity such as driving. This right to anonymity with regard to the state is a crucial privacy right. But since we are required to identify ourselves to airlines as a condition of air travel and since section 4.82 would give the RCMP unrestricted access to the passenger information obtained by airlines, this would set the extraordinarily privacy-invasive precedent of effectively requiring compulsory self-identification to the police.

I am prepared, though I seriously doubt its effectiveness, to accept this as an exceptional measure that can be justified in the wake of September 11 for the limited and specific purposes of aviation security and national security against terrorism. But I can find no reason why the use of this de facto self-identification to the police should be extended to searching for individuals who are of interest to the state because they are the subject of warrants for *Criminal Code* offences unrelated to terrorism. That has the same effect as requiring us to notify the police every time we travel, so that they can check whether we are wanted for something.

If the police were able to carry out their regular *Criminal Code* law enforcement duties without this new power before September 11, they should likewise be able to do so now.

If we accept, instead, the principle that air travellers within Canada can now in effect be forced by law to identify themselves to police for scrutiny against lists of wanted suspects, then there is nothing to prevent the same logic from being applied in future to other modes of transportation. Particularly since this provision might well discourage wanted individuals from travelling by air, why not extend the same scrutiny to train travellers, bus passengers or anyone renting a car?

Indeed, the precedent set by this provision could ultimately open the door to practices similar to those that exist in societies where police routinely board trains, establish roadblocks or stop people on the street to check identification papers in search of anyone of interest to the state.

This is why I have recommended amending the bill to remove all reference to warrants and thus limit the police to using this passenger information only to watch for individuals who are of concern specifically on grounds of anti-terrorism and national security.

When the Government reintroduced this legislation as Bill C-17, it made a number of changes. But my recommendations regarding section 4.82 were ignored. Instead, the Government made two changes that are at best cosmetic, and that appear aimed more at misleading Canadians than at addressing the real issues that are at stake.

The Government now proposes to have regulations limiting slightly the *Criminal Code* offence warrants for which the RCMP will be searching. But this does nothing to address the fundamental point of principle that the police have no business using this extraordinary access to personal information to search for people wanted on warrants for any offences unrelated to terrorism.

As well, in the new bill the Government has removed the "identification of persons for whom a warrant has been issued" as a "purpose" for accessing passenger information under the legislation. But this is meaningless, since the RCMP would remain empowered to match this information against a database of persons wanted on warrants and to use such matches to bring about arrests.

Senior Government officials have repeatedly told me that the reference to warrants is necessary, because otherwise the RCMP would be powerless to act if they "incidentally" came upon the name of a dangerous wanted criminal while scanning a passenger list for possible terrorists. This argument is totally unpersuasive for two reasons.

First, if RCMP officers are to examine passenger information for the sole stated purpose of looking for terrorists and security risks, they shouldn't be checking passenger names against the huge general CPIC database, which contains a very wide variety of information including the names of people wanted on all sorts of warrants completely unrelated to terrorism. They should be looking for matches against the much more specific database that is limited to information only on known or suspected terrorists and other individuals identified as security risks.

To say that trolling in CPIC might cause the RCMP to "incidentally" find individuals wanted on warrants for *Criminal Code* offences, is like saying that there is something "incidental" about tossing a fishing line into a pond stocked with trout and pulling out a trout.

Second, my legal advisors have confirmed that peace officers including the RCMP have a well-established Common Law power – indeed a duty – to take appropriate action to apprehend any potentially dangerous individual they discover to be wanted on a warrant. The reference to warrants in section 4.82 of Bill C-17 is therefore quite redundant and unnecessary – unless, of course, the RCMP are to make a systematic practice of searching passenger information for individuals wanted on outstanding warrants, contrary to the stated purpose of giving them access to this information.

"THE INTERCEPTION AND MONITORING OF PRIVATE COMMUNICATIONS IS A HIGHLY INTRUSIVE ACTIVITY THAT STRIKES AT THE HEART OF THE RIGHT TO PRIVACY.

The "Lawful Access" Initiative

Under the "Lawful Access" proposals that have been put forward jointly by the Minister of Justice, the Solicitor General and the Minister of Industry, the Internet activities and cellular phone communications of all law-abiding Canadians would be subject to unprecedented scrutiny by the state.

I have responded formally, publicly and in detail to these proposals, and will not do so again here. But I have received absolutely no indication that the grave privacy concerns I have expressed will be heeded, and I have considerable reason to fear that the Government intends to simply press ahead.

The interception and monitoring of private communications is a highly intrusive activity that strikes at the heart of the right to privacy. If Canadians can no longer feel secure that their Web surfing and their electronic communications are indeed private, this will mark a grave, needless and unjustifiable deterioration of privacy rights in our country.

The Government has presented no evidence to demonstrate why the massive new intrusions it proposes are necessary.

I recognize that new information technologies may pose a challenge to conventional interception and surveillance techniques used by police forces and national security agencies. It appears reasonable that law enforcement and national security agencies should have the same ability to intercept and monitor e-mail and cellular telephone communications, with the same kind of judicial authorization based on the same criteria, as is now the case with regard to letter mail and conventional telephone communications.

But agents of the state in Canada cannot order Canada Post to photocopy the address on every envelope we send, nor can they order bookstores to keep a record of every book we buy, let alone of every page of every magazine we leaf through. There is no reason why they should be able to exercise such powers with regard to every e-mail someone sends or every Web site he or she visits.

I do not see any reason why e-mails should be subject to a lower standard of privacy protection than letters or telephone calls. And I do not see why Internet browsing should be subject to a lower standard of protection than book purchasing or researching in a reference library. Canadians should not be subject to greater state monitoring or scrutiny just because they choose to use new communication technologies.

In a free and democratic society like Canada, the interception and monitoring of private communications carries extraordinarily strong symbolic and psychological implications, in addition to the obvious practical ones. Dramatically increasing that interception and monitoring, without any clearly demonstrated need or justification, is unacceptable.

I CAN FIND NO JUSTIFICATION FOR A NATIONAL IDENTITY CARD, ESPECIALLY SINCE IT IS ABSOLUTELY USELESS AS AN ANTI-TERRORIST MEASURE.

Identity Cards

It is a matter of very considerable dismay that Citizenship and Immigration Minister Denis Coderre, presumably on behalf of the Government, is pressing for a "debate" on establishing a mandatory national identity card, complete with biometric identifiers, for all Canadians.

Given the Government's current behavior on other privacy matters, it is difficult to avoid fearing that this means that it wishes to introduce such a card.

That would be another huge blow to privacy rights. In Canada, we are not required to carry *any* identification – let alone to identify ourselves on demand – unless we are carrying out a licensed activity such as driving. Introducing a national identity card, even if it were "voluntary" at first, would push us toward becoming the kind of society where the police can stop anyone on the street and demand, "Your papers, please."

The notion of the Government of Canada fingerprinting or eyeball-scanning every citizen for such a card is, of course, all the more abhorrent.

I can find no justification for a national identity card, especially since it is absolutely useless as an anti-terrorist measure. As the perpetrators of the September 11 attacks demonstrated, terrorists are not necessarily previously identifiable as such. Every citizen would be able to obtain and display an identity card, regardless of his or her possible terrorist proclivities, but of course it wouldn't list occupation as "terrorist." And short-term visitors to Canada wouldn't have such a card at all.

Rather than a "debate" about a grave and needless intrusion, Canada needs clear acknowledgement by the Government that the fundamental privacy right of anonymity as we go about our day-to-day lives is too important to abrogate for no apparent reason.

Video Surveillance

I have been trying for more than a year to persuade the Government to direct the RCMP to stop its continuous video surveillance of law-abiding citizens on a public street in Kelowna, British Columbia.

I believe that general video surveillance of our public streets and public gathering places by the police or other public authorities is an enormous threat to the fundamental human right of privacy in our society.

We have the right as Canadians to walk along our public streets without being systematically observed by police. If we lose that, we lose a crucial part of our privacy and our freedom.

Last March, I sought the advice of retired Supreme Court Justice Gérard La Forest, who wrote many of the Supreme Court's most important decisions on privacy rights. Mr. La Forest advised me that, in his learned opinion, what the RCMP is doing in Kelowna

is not only a serious violation of privacy rights, but is also a clear contravention of the *Canadian Charter of Rights and Freedoms*.

I made that legal opinion public last April, and it too was ignored by the RCMP and the Government. Since as Privacy Commissioner I am mandated by Parliament to oversee and defend the privacy rights of Canadians, and since I have the strongest possible reason to believe that what the RCMP is doing in Kelowna not only violates privacy rights in general but is unconstitutional, my only remaining recourse is to ask the courts to put a stop to it.

Accordingly, in July I initiated in the Supreme Court of British Columbia in Kelowna, an action to declare the RCMP's video surveillance activities in Kelowna unconstitutional as a violation of the *Canadian Charter of Rights and Freedoms* and international covenants.

Remarkably, the Government has taken the position that it challenges my right to take this action. It takes the position that as Privacy Commissioner I am a "statutory body" limited to doing only what is expressly spelled out in the *Privacy Act*.

My legal advisors inform me that they are confident that this position is not correct in law. But I have strong reason to believe that if my right to initiate this *Charter* challenge is upheld by the court, the Government intends to file a series of appeals with a view to preventing this important case from being heard on its merits for years to come.

That would be reprehensible. At a time when video surveillance of public streets is becoming a fad that appeals to many municipalities across Canada, Canadians are entitled to have this important question about their privacy rights under the *Charter* adjudicated without delay. As well, police forces and municipalities across the country should themselves not be subjected to prolonged and needless uncertainty about the constitutional legality of what they are contemplating. They want and need a court decision.

I have therefore repeatedly asked the Minister of Justice and Attorney General, Mr. Cauchon, to withdraw this procedural objection and allow the case to be promptly determined on its merits. I have recently been informed that he refuses to do this.

Instead the Government, through the Minister of Justice, is taking the extraordinary position that the Privacy Commissioner of Canada should not have the right to ask the courts to determine whether a grave intrusion on privacy violates the privacy protections in the *Canadian Charter of Rights and Freedoms*.

I urge the Government to reconsider.

> 'The United States made us do it' cannot be a sufficient or acceptable justification for the Government to intrude on a fundamental right of Canadians.

With regard to all these initiatives except street video surveillance, Government officials have repeatedly told me privately that pressure from the United States government is a strong motivating factor.

Let me be blunt: "The United States made us do it" cannot be a sufficient or acceptable justification for the Government to intrude on a fundamental right of Canadians.

Canada is a sovereign country.

Throughout our history, there have been important instances where Canada has found it necessary to take a position different from that of the United States on matters involving rights or values. It is surely no exaggeration to say that if our leaders had instead consistently succumbed to U.S. pressures to adopt that country's approaches as our own, there would today be no distinct Canada as we know it.

The same is true with regard to appropriate respect for fundamental rights in the wake of September 11. If the U.S. government is indeed exerting pressure on Canada to take steps that cannot be justified on their merits in accordance with our Canadian values and rights, then Canadians are entitled to expect that the Government will remain steadfast in meeting its responsibilities rather than trample on their rights out of fear of U.S. retaliation.

Canadians are entitled, as well, to expect that the Government will think very carefully and critically before accepting the U.S. premise that we are all "at war" against terrorism and that it is therefore reasonable to impose wartime restrictions on privacy and other rights.

The difficulty is that terrorism is not an enemy, but a phenomenon. Wars that are fought between nation-states, or even civil wars that are fought within a country, are finite. They may drag on for a long time, but eventually someone wins and someone loses or a stalemate is identified, and the terms of peace are established.

But if we apply the premises of war to the challenges of dealing with terrorism, we will by definition be committing ourselves to a "war" with no possible end – because there is no single, definable enemy. Any group of individuals, or even any single individual, that is willing to commit public mayhem in support of any particular cause is thereby a terrorist. And so for every particular group or faction of terrorists that is neutralized, another one may readily spring up.

This means that there can never be a moment when it will be possible to declare a definitive victory in a "war" against terrorism. In fact, such a "war" will be eerily reminiscent of Orwell's *1984*, which takes place against the background of a mysterious chronic war in which it is never clear just who the enemy is or who is winning or losing.

We need to recognize, therefore, that any intrusions or limitations on the fundamental human right of privacy that are imposed as a purported wartime measure against terrorism will likely never be rescinded. What we are confronting is the prospect of a permanent redefinition of Canadian society.

And what will this redefinition achieve in terms of protecting us?

The reality is that there are no security measures that can provide complete protection against murderous individuals or groups who are willing to lose their own lives to make their point. Even the most repressive, authoritarian regimes have not been able to immunize themselves fully against terrorism. At the same time, we also need to keep the risks in perspective: In any scenario, the average Canadian is far more likely to come to harm in a traffic accident than at the hands of terrorists.

This is not to suggest that we should take a cavalier approach to terrorism, but rather that we must take a balanced one.

When people are worried about their safety, when we have seen the horrors of which today's breed of terrorists are capable – and there may be more – it's easy to lose perspective. It's easy to fall into the trap of thinking that security is all that matters and that human rights such as privacy are a luxury.

But such extremes can only reward and encourage terrorism, not diminish it. They can only devastate our lives, without commensurately safeguarding them.

Of course we all want to be safe. But we could be safer from terrorism – perhaps – if we permanently evacuated all the high-rise office towers, if we closed down the subways, if we forever grounded all airplanes.

Yet no reasonable person would be likely to argue for adopting such measures. We'd say, "We want to be safe, yes – but not at the price of sacrificing our whole way of life."

The same reasoning should apply, in my view, to arguments that privacy should indiscriminately be sacrificed on the altar of enhanced security.

The essence of terrorism is the impact it is intended to have on those who witness it – the capacity to frighten, to demoralize, to sap the will of a society to resist whatever it is that the terrorists want.

In the case of the September 11 breed of terrorists, by all accounts it is the whole nature of American society, and by extension of all our Western societies, that they seek to attack and undermine. Our freedoms and values, very much including privacy, are precisely the target.

To keep that from becoming a reality for Canada, we must guard against falling prey to the illusion that wholesale erosion of privacy is a reasonable, necessary or effective way to enhance security.

> We must guard against the eagerness of law enforcement bodies and other agencies of the state to use the response to September 11 as a Trojan horse for acquiring new invasive powers.

We must guard against the demonstrated tendency of the Government to create new databases of privacy-invasive information on justified, exceptional grounds of enhancing security, and then seek to use that information for a whole range of other law enforcement or governmental purposes that have nothing to do with anti-terrorism – simply because it's there.

And we must guard against the eagerness of law enforcement bodies and other agencies of the state to use the response to September 11 as a Trojan horse for acquiring new invasive powers or abolishing established safeguards simply because it suits them to do so.

Perhaps it will be necessary to accept some new intrusive measures to enhance security. But these choices must be made calmly, carefully and case by case. The burden of proof must always be on those who suggest that some new intrusion or limitation on privacy is needed in the name of security.

I have suggested that any such proposed measure must meet a four-part test:

It must be demonstrably necessary in order to meet some specific need.

It must be demonstrably likely to be effective in achieving its intended purpose. In other words, it must be likely to actually make us significantly safer, not just make us feel safer.

The intrusion on privacy must be proportional to the security benefit to be derived.

And it must be demonstrable that no other, less privacy-intrusive, measure would suffice to achieve the same purpose.

Necessity, effectiveness, proportionality, and lack of a less privacy-invasive alternative – this is the four-part test that I believe can allow us to take all appropriate measures to enhance security, without unduly sacrificing privacy. It is a test on which I believe all of us – every Canadian, and particularly every Member of Parliament and Senator, of every party and every political philosophy – must resolutely insist.

One of the clearest lessons of history is that the greatest threats to liberty come not when times are tranquil and all is well, but in times of turmoil, when fidelity to values and principle seems an extravagance we can ill afford. History also teaches us that whenever we have given in to that kind of thinking, we have lived to regret it.

At the time, the loss of freedom might seem small, trivial even, when placed in the balance of the security we seek. And yet these incremental threats are the ones we must be most vigilant in resisting. The 18th Century political philosopher Edmund Burke understood this danger when he wrote, "The true danger is when liberty is nibbled away, for expedience, and by parts."

U.S. Supreme Court Justice Thurgood Marshall eloquently made the same point much more recently when he said: "History teaches that grave threats to liberty often come in times of urgency, when constitutional rights seem too extravagant to endure."

We are now living in such a time. Canada has, over the course of its history, developed a very healthy balance between the powers of the state and the rights of the individual. Our crime rates have been comparatively low and our social order has been strong, while individual freedom and diversity have flourished to a degree that is the envy of much of the world. That is why immigrants from so many other societies have chosen to make Canada their home.

But now we face having that successful balance changed, by having Canada transformed into a society where the state is much more intrusive and where individual rights and freedoms are correspondingly reduced. And we face having this transformation occur without the analysis, debate or even understanding that it deserves.

Sadly, most of the ministers who are making these decisions are not thinking sufficiently about the deeper implications of what they are doing. While I am continuing to maintain dialogue with the relevant officials in pursuit of appropriate changes, at the time this Report goes to press no discernible progress has been made.

Even with the help and support of my provincial and territorial colleagues, other privacy advocates and many thoughtful members of the news media – to all of whom I am profoundly grateful – as an ombudsman I do not have the power to stop what the Government is doing in its unprecedented assault on privacy.

That power lies in Parliamentary insistence and public outcry. It is my hope that these will be exercised with the greatest urgency. It is also my hope that, even at this late moment, the Government will have the courage and the good sense to recognize that there is no shame in rethinking and revising insufficiently-considered policies. There can be shame only in insisting, instead, on treading needlessly on a fundamental right of Canadians.

For my part, my role and my duty are to bear true witness to what is taking place, and to fight against it with every appropriate means available to me. This I will continue to do ceaselessly, and with all the vigour at my disposal.

Part One
Report on the *Privacy Act*

Introduction

The *Privacy Act* protects individuals' privacy with respect to personal information held by federal Government institutions.

The *Act*, which has been in force since 1983, governs how federal institutions collect, use, disclose and dispose of personal information, and gives people the right to access and request corrections to their personal information.

As Privacy Commissioner, I receive and investigate complaints from individuals who believe their rights under the *Act* have been violated. I can also initiate a complaint and an investigation myself, in any situation where there are reasonable grounds to believe the *Act* has been violated.

First and foremost, I am an ombudsman, and whenever possible, complaints are resolved through mediation and negotiation. But I also have broad powers of investigation under the *Act*. As Privacy Commissioner I can subpoena witnesses, compel testimony and enter premises to obtain documents and conduct interviews. Obstructing one of my investigations is an offence under the *Act*. Although the *Act* does not include the power to order compliance, I can recommend changes to the way Government institutions handle personal information, based on my findings.

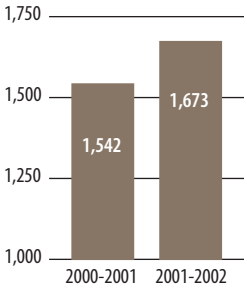
As well, I have a mandate to conduct periodic audits of federal institutions to determine their compliance with the *Act* and, on the basis of my findings, I can recommend changes.

The *Act* requires me to submit an Annual Report to Parliament on the activities of my Office in the previous fiscal year. This current report covers the period from April 1, 2001 to March 31, 2002 for the *Privacy Act.*

Investigations

My Investigations Branch investigates individuals' complaints under section 29 of the *Privacy Act* (and under section 11 of the *Personal Information Protection and Electronic Documents Act*, which I will discuss later in the report).

Complaint Investigations Closed
April 1, 2001 to March 31, 2002



Through these investigations, I determine whether individuals' privacy rights have been violated or whether they've been properly accorded access to their personal information. Where people's privacy rights have been violated, I look for ways to provide redress for them and to prevent violations from happening again.

I have authority under the *Act* to administer oaths, receive evidence and enter premises where appropriate. I can also examine or obtain copies of records found on any premises.

To date, we have had voluntary co-operation and all complaints under the *Privacy Act* have been resolved without our having to use these formal investigative powers.

Complaints under the *Privacy Act*

During the fiscal year of April 1, 2001 to March 31, 2002, we received a total of 1,213 complaints under the *Privacy Act*. Of those, 45 per cent concerned denial of access to personal information, 20 per cent were related to issues of collection, use, disclosure, retention and disposal of personal information, and the remaining 35 per cent concerned failure to respond to an access request within the legislated timeframes set out in the *Act*.

Investigations staff completed investigations of 1,673 complaints, an increase of 8 per cent over the previous year. Of those, 703 dealt with denial of access, 397 concerned issues related to collection, use, disclosure, retention and disposal of personal information, 571 were about lack of timeliness in responding to requests to obtain access to personal information and two dealt with other matters including an allegation of retaliation against an individual for submitting an access request. These complaints were concluded as follows:

Not well-founded:	445
Well-founded:	668
Well-founded/Resolved:	91
Resolved:	26
Settled during the course of the investigation:	344
Discontinued:	99

Definitions of Findings under the *Privacy Act*

Not well-founded: A finding that a complaint is *not well-founded* means that the investigation uncovered no evidence to lead me to conclude that the Government institution violated the complainant's rights under the *Privacy Act*.

Well-founded: A finding that a complaint is *well-founded* means that the Government institution failed to respect the *Privacy Act* rights of an individual. This would also be my finding in a situation where the Government institution refuses to grant access to personal information, despite my recommendation that it be released. In such a case, my next step could be to seek a review by the Federal Court of Canada.

Well-founded/Resolved: I will find a complaint to be *well-founded/resolved* when the allegations are substantiated by the investigation and the Government institution has agreed to take corrective measures to rectify the problem.

Resolved: *Resolved* is a formal finding that reflects my role as an ombudsman. It's for those complaints where *well-founded* would be too harsh to fit what essentially is a miscommunication or misunderstanding. It means that my Office, after a full and thorough investigation, has helped negotiate a solution that satisfies all the parties.

Settled during the course of the investigation: This is not a formal finding but an acceptable means to dispose of a complaint when the investigation is completed, and the complainant is satisfied with the efforts of my Office and doesn't wish to pursue the issue any further. The complainant retains the right to request a formal finding. When that happens, the investigator re-opens the file, and submits a formal report, and I report the findings in a letter to the complainant.

Discontinued: This means that the investigation was terminated before all the allegations were fully investigated. A case may be *discontinued* for any number of reasons – for instance, the complainant may no longer be interested in pursuing the matter or cannot be located to provide additional information critical to reaching a conclusion. I don't issue a formal finding in discontinued complaints.

In my report last year, I expressed concerns that a few Government departments and agencies – most notably, Correctional Service Canada (CSC), the Department of National Defence (DND), the Canada Customs and Revenue Agency (CCRA) and Human Resources Development Canada (HRDC) – had been particularly lax in responding to access requests in a timely fashion.

There are indications that these departments and agencies are improving their turnaround times as a result of special measures they have put in place to deal with their backlogs. We received fewer time-limit complaints against these institutions this past year, with the exception of DND. This fact may indicate improved performance, or simply that they received fewer requests last year and therefore fewer dissatisfied individuals turned to my Office for assistance. Regardless, most of the time-limit complaints we investigated against CSC, DND and HRDC were deemed well-founded, a clear indication that these institutions are still not meeting their obligations under the *Privacy Act*.

Summary of Select Cases Under the *Privacy Act*

Departments accountable for information collected under contract

Despite past reminders, some departments still neglect to ensure that personal information collected under the contracts they negotiate with outside contractors is managed in accordance with the fair information principles of the *Privacy Act*.

Those principles require Government institutions that are subject to the *Act* to include provisions in contracts that:

- Define ownership of the information – that is, all information collected as part of the contract belongs to the contracting department or agency and should be turned over to it at contract end;
- Recognize individuals' rights of access to their personal information collected during the contract;
- Restrict further uses of the personal data;
- Protect the information against unauthorized disclosure;
- Establish retention and disposal criteria; and
- Ensure the department's ability to audit compliance of the contractor's management of the information collected.

In one case investigated this past year, an employee of Human Resources Development Canada (HRDC) complained that she did not receive all of her personal information gathered by an independent contractor hired by the department to conduct a workplace assessment. The employee was particularly interested in obtaining access to any mention of her by other staff in the contractor's interview notes and questionnaires.

When interviewed, the contractor admitted to destroying all the information except the report she produced for HRDC. She did this in part because she had promised confidentiality to the individuals she interviewed, indicating that their statements would not be released, and the contract signed with HRDC did not specify otherwise.

Although HRDC's policies and procedures on contracting out to third parties specify that all the provisions of the *Privacy Act* are to be respected, the contractor in this case was not aware of HRDC's obligations under the *Act* to retain the information or grant individuals access to their own information. Contractors (as well as employees conducting similar administrative investigations) must be informed that they cannot promise confidentiality and, prior to taking statements about an individual, they must inform witnesses that their statements constitute the other individual's personal information for which rights of access are provided by the *Privacy Act*. The witness then has a choice as to whether or not to provide a statement that would include information about another individual.

I concluded that the complaint was well-founded and HRDC was accountable for the work done under the contract. The contractor's failure to retain the information in essence resulted in the complainant being denied an opportunity to obtain access to her own information.

In a case against the Department of National Defence, a military officer sought my assistance in getting access to his medical records, including the notes of an independent medical specialist the department hired to provide an opinion based on his review of the complainant's medical file. When the officer submitted his access request, the department released the medical records in its file, but did not release the specialist's notes from the independent review.

When I investigated the matter, I learned that no effort had been made to get the information from the specialist. I interviewed the specialist and reviewed his notes, which clearly contained personal information about the complainant. The specialist claimed that he had not been told that the information he gathered as part of his review belonged to the department and that he should also supply a copy of all the information from his file to the department for inclusion in its records. Nevertheless, the

specialist willingly provided a copy to the department so that it could in turn release it to the complainant. The complainant was pleased to receive the information and did not request that we pursue the matter further.

These two cases serve to remind federal departments and agencies that any contracts they enter into that require the collection of personal information must also include appropriate clauses to satisfy the provisions of the *Privacy Act*. Individuals should be able to access their own information whenever it is requested.

RCMP charges fee for traffic analysis report

A British Columbia man asked the Royal Canadian Mounted Police (RCMP) for a copy of a traffic analysis report prepared following an investigation of a traffic accident in which he was involved. The report attempted to reconstruct the circumstances surrounding the accident, and the man wanted to use it to support a civil claim. When he requested a copy of this report informally from the RCMP detachment where it was prepared, he was told there was a $500 fee. He then formally requested it under the *Privacy Act* but was refused on the basis that it was exempted under section 22(1)(a) of the *Act*. Section 22(1)(a) allows an investigative body such as the RCMP to deny access to information about a lawful investigation that is less than 20 years old. In his letter of complaint, the man correctly asked how the information could be available if he paid the $500 fee but not under the *Privacy Act*, to which no fees apply.

I determined that the RCMP detachment's response to the informal request was based on an established fee schedule. When the *Privacy Act* request was received at the RCMP's Access to Information and Privacy Unit in Ottawa, it confirmed that the accident was still under investigation. The RCMP routinely refuses access to information related to ongoing investigations. The unit subsequently informed the complainant that the report was exempted in its entirety under section 22(1)(a) of the *Act*.

However, upon further inquiries, I learned that in August 2000 the RCMP had issued a bulletin to all detachments in British Columbia that no fee should be collected for these reports. This decision followed a 1998 Supreme Court of British Columbia ruling in a case against the RCMP as the municipal police force under contract to the province. The Court ruled that the fee charged by the RCMP for a traffic analysis report was in essence a tax disguised as a user fee, and therefore was without any legislative authority.

As a result of our intervention, the RCMP provided the man with his own personal information in the report, which was all he was entitled to receive under the *Privacy Act*.

DND improperly retains, uses information about pardoned convictions

I investigated complaints from two Canadian Forces members who felt their privacy had been violated when the Department of National Defence (DND) kept information on its files related to their criminal convictions and subsequently used that information to deny them employment opportunities.

In the first case, the member had been selected for a posting with a United Nations tour in the Middle East, but just prior to his departure the posting was cancelled by his base commanding officer. I learned that DND's Military Police discovered the member had been charged with impaired driving shortly before his planned departure date and had reviewed its records to determine whether the man had any other charges against him. It found seven references to other criminal offences and forwarded this information to the base commanding officer. When the commanding officer saw the record, he decided against sending the member overseas.

I determined that two of the offences should have been purged from the member's file since he had received a pardon for them. The Pardons and Clemency Division of the National Parole Board had notified DND of these pardons and of the department's requirements under the *Criminal Records Act* to segregate its records related to these offences from other criminal records in its custody. DND complied but only insofar as reference to the convictions was concerned – all the facts related to the charges that led to these two convictions remained on file.

Unfortunately, when only the reference to a conviction is removed from a record, what remains can be misleading to anyone who has access to that information. I therefore reminded DND that under the *Privacy Act* it is required to ensure that personal information used for an administrative purpose – that is, in a way that directly affects the individual to whom it relates – is accurate, up-to-date and complete.

As a result of my efforts, DND agreed to amend its policy on the retention of information about pardoned convictions to conform with both the *Privacy Act* and the *Criminal Records Act*.

In the second case, an individual obtained information that led him to believe DND used information about his convictions under the *National Defence Act* to reject his application for re-engagement in the Canadian Forces, despite the fact that he had been granted a pardon.

When I investigated the matter, I confirmed that DND had indeed used this information in its assessment of his application. I also confirmed with the Pardons and Clemency Division of the National Parole Board that it had granted a pardon to the individual but

had neglected to inform DND. I therefore asked the National Parole Board to send appropriate notifications to DND and the National Archives, the current custodian of the individual's military records, so that they could amend his records as required.

CMHC's demand for tax information inappropriate

The president of a consulting firm complained that Canada Mortgage and Housing Corporation (CMHC) had asked for an excessive amount of personal information from sole proprietors and partnerships as proponents in a Request for Proposal (RFP) process. If the lead proponent turned out to be a sole proprietor, that individual was required to provide, among other things, copies of his/her income tax returns for the last three years and a statement of net worth.

I discussed the RFP process with CMHC in depth. It was adamant that it was necessary to obtain financial information from a lead proponent when there was a high degree of risk associated with procurement and that it must ask for detailed information from a sole proprietor just as it did with any other type of business. It argued that, for a sole proprietor, unlike for a corporation, there was little comprehensive financial information that could be used to conduct an accurate risk assessment and that the information it was requesting was the best and most accurate it could get.

I agreed that the financial viability of a lead proponent had to be assessed to minimize the organization's exposure in high-risk cases. However, I did not understand how this objective was achieved by assessing income tax information for a three-year period. An individual may have had substantial revenue over three years but income tax information would not reveal how the individual disposed of that revenue. A proprietor may have had three difficult years but could still support the financial strains of a contract. An individual may also have substantial assets in property or non-interest bearing investments that are simply not reflected in income tax documents.

Section 4 of the *Privacy Act* provides that personal information collected by a Government institution must relate directly to an operating program or activity of the institution. Because I did not believe that income tax information was of material assistance in helping CMHC to assess the quality of a sole proprietor's RFP proposal, I could not conclude that CMHC's request for that information met the requirements of section 4. As a result of my investigation, CMHC has amended its procurement policy and has discontinued the practice of requesting income tax returns and statements of net worth from sole proprietors.

It is unacceptable to me that Canadian citizens should have to provide copies of their personal income tax returns to do business with the Government. Under the *Income Tax Act*,

individuals must divulge a vast amount of personal information when completing their income tax returns, including a good deal of personal information about family members. The income tax process is extraordinarily intrusive and the use of personal information collected for income tax purposes must, in my view, be strictly confined to purposes that are regulated. At a time when Canadians are increasingly concerned about the erosion of their personal privacy, I find it untenable that an income tax return can be demanded from an individual for a purpose other than that required by law. Canadians should never be required to compromise a fundamental right in order to do business with the Government.

Ultimately, CMHC agreed with my finding and halted the practice. Although my investigation focused on CMHC practices, I was aware that other federal Government departments and agencies followed similar practices. I therefore wrote to the Deputy Minister for Public Works and Government Services Canada, and to the Secretary of the Treasury Board and the Comptroller General of Canada, seeking their assistance to ensure that this practice is discontinued throughout the federal Government. The Treasury Board agreed with my view. It indicated that the practice was not Government policy and that the matter would be raised with other departments and agencies. I have also been informed by Public Works and Government Services that it will discontinue the practice.

Inappropriate monitoring of employees' e-mail accounts

I investigated several complaints from individuals questioning managers' authority to search Government e-mail accounts during the course of administrative investigations.

In one instance, two employees at the Immigration and Refugee Board (IRB) alleged that local management improperly retrieved copies of confidential e-mail messages they had written each other regarding a *Privacy Act* complaint to this Office by one of the employees.

By way of background, one of the employees had discovered performance evaluations about several of her co-workers on the local computer network and immediately notified her union's representative, another IRB employee. The representative obtained copies of the evaluations to support his complaint to this Office about the improper disclosure of personal information.

My investigation of that complaint determined that the IRB had not taken adequate steps to restrict access to the information and I concluded that the complaint was well-founded.

Management of the IRB fixed the computer glitch that had created the problem as soon as it was notified of the substance of this complaint. Management also initiated an inquiry

into the incident to establish whether any disciplinary action should be taken against the employee for disclosing the evaluations to the union representative. On instruction, the local information technology manager searched and retrieved some e-mail communications concerning the incident between the employee and the union representative.

The IRB did not have a formal policy on the use of electronic networks at the time of this incident. In the absence of a policy, it is guided by Treasury Board policies dealing with employees' expectation of privacy and the statement of authorized uses. The IRB stated that it supports the principle that access to an employee's e-mail without consent is justified only in extreme situations, for example in situations involving a criminal or security infraction, and only after proper authorization from senior management.

However, in the case in question, prior to conducting the search of the electronic system, the IRB was already well aware of the employee's actions and her contact with the union representative. Its decision to retrieve their e-mail messages was not based on any concern that they were improperly using the system. Rather, the primary purpose was to conduct an internal disciplinary inquiry.

My view was that it was unnecessary for the IRB to retrieve the e-mail exchanges to determine if disciplinary action against the employee was warranted and therefore its actions could not be justified under the *Privacy Act*. I recommended that the IRB proceed quickly to complete its disciplinary review and that it publish a policy, similar to Treasury Board's, governing the use of its electronic networks.

In another case, a Human Resources Development Canada (HRDC) employee complained that her supervisor retrieved personal e-mails she sent from her home to a co-worker and improperly used them in the course of an internal investigation into allegations that had been made against her by her union local.

I established that HRDC's local management was investigating an allegation that the employee interfered with a grievance process. During the investigation HRDC searched its Internet network database for any e-mail exchanges she might have had with a particular co-worker about the grievance. HRDC made no effort to obtain the consent of either individual before searching the co-worker's office e-mail account. One personal message from the complainant to the co-worker contained a reference to the grievor by name but nothing else related to the grievance. The message was otherwise predominantly personal in nature. Yet the department subsequently used it during its investigation process.

I accept that there may be occasions that would justify an employer's decision to review an employee's Internet network account and then use that information in a disciplinary process. However, this was not such an occasion. There was no evidence to suspect that the co-worker was in any way implicated in the internal investigation that would lead HRDC to search her account. By collecting the complainant's personal e-mail exchanges with the co-worker without consent, and subsequently using it to investigate the complainant, HRDC violated her *Privacy Act* rights.

Man denied access to his information following war crimes investigation

A European immigrant, now a Canadian citizen, requested my intervention after the Royal Canadian Mounted Police (RCMP) repeatedly denied him access to its investigation file of his involvement in Nazi activities in Jewish death camps during World War II.

The man was denied entry into the United States in 1990 when his name appeared in a database containing information gathered by the U.S. Justice Department's Office of Special Investigations (OSI). The database contained the names of all members of a Nazi unit, regardless of rank, occupation or activity. The OSI then asked the RCMP to investigate the extent of the man's involvement in the Nazi unit. During the investigation, carried out jointly by the RCMP's War Crimes Section and Justice Canada's Crimes Against Humanity and War Crimes Section, the RCMP interviewed the man about the U.S. allegations.

Over a period of several years, he attempted to obtain information from the RCMP about its investigation so that he could take appropriate action to clear his name, but was always rebuffed. The RCMP claimed it was still looking into the allegations and releasing anything from its files might jeopardize the integrity of its investigation.

He requested a copy of the file again in 2000 after he received correspondence from the Department of Justice advising him that its joint investigation with the RCMP was concluded and the file had been closed. The RCMP refused again, saying the file was exempted in its entirety under section 22(1)(a) of the *Privacy Act*, and verbally told him that the case was still ongoing. He then complained to my Office.

When a privacy officer of my Investigations Branch reviewed the information withheld by the RCMP, he noted that some of the information was almost 60 years old and therefore did not qualify for exemption under the provision cited by the RCMP. The RCMP then considered applying another exempting provision, section 22(1)(b), but to do so properly, the RCMP would have to demonstrate the injury that would likely occur to its investigation if the information were released.

Since the investigation was already concluded, the privacy officer questioned how disclosure of the information could cause injury. The RCMP maintained that its investigation was not yet finalized even though there had been no activity on the file since 1997.

After the privacy officer confirmed with the Department of Justice's Crimes Against Humanity and War Crimes Section that the case was closed for lack of evidence to proceed, the RCMP conceded and agreed to disclose information from its file.

Disclosure of information during appeal should be limited

Several individuals who had appealed a Human Resources Development Canada (HRDC) decision to recoup an overpayment of employment insurance (EI) benefits, complained that personal information was improperly disclosed during the appeal process.

The complainants were among over 200 individuals who received EI benefits after losing their employment. Because they filed a grievance about their termination that resulted in being awarded severance packages, HRDC commenced action to recoup the EI benefits the individuals received for the period they were covered by the severance package. They appealed HRDC's decision to the EI Board of Referees.

As part of the appeal process, HRDC's local office sent a disclosure package to each of the appellants. Each package was to contain information related to that particular individual's appeal. However, one complainant's package included a document that contained the names, addresses, phone numbers and Social Insurance Numbers (SINs) of 14 other individuals involved in the appeal. When he informed HRDC of the impropriety, it reviewed its records and established that only two of the appellants had received this document.

HRDC immediately took steps to retrieve the document from both individuals and replace it with a properly vetted copy. It also contacted by phone or letter the others whose personal information had been inadvertently revealed and explained the error.

After they lost their appeal, the appellants sought a second-level review that required HRDC's district office to send each appellant a disclosure package related to that particular individual. Once again, one of the complainants got the identical document he had received previously, disclosing personal information about 14 other appellants. It was this second disclosure that prompted the complaint to me.

I was troubled that HRDC's district office would disclose the same information as the local office, despite the admission that the disclosure had been made in error. Clearly, the document should have been properly vetted by the local office the first time it was sent. The district office compounded this error when it sent the same information a second time, which it felt was required to ensure procedural fairness. I concluded that HRDC had violated the complainants' rights under the *Privacy Act*.

I therefore recommended that HRDC build in procedures that would respect procedural fairness throughout the various levels of the EI appeals process while at the same time recognizing its obligations under the *Privacy Act* to disclose personal information only when it is directly relevant to the appeal at hand.

In another case, a woman complained that information she had provided to HRDC to support her claim for a survivor's benefit under the *Canada Pension Plan* was disclosed to family members of her deceased common-law husband. HRDC had received applications from both the complainant and the deceased's wife by marriage, and ultimately gave the benefit to the common-law wife. The legal wife filed an appeal of HRDC's decision with the Office of the Commissioner of the Review Tribunals (OCRT).

The *Review Tribunal Rules of Procedure* require HRDC to convey to the OCRT copies of any documents relevant to its decisions. Under the same *Rules*, the OCRT must share copies of these same documents with the appellant. Therefore, the OCRT provided copies of all documents it received from the deceased's common-law wife. These documents contained information the common-law wife had given to HRDC to demonstrate her relationship with the deceased and her entitlement to the benefit – including her SIN, her application for Old Age Security, a copy of a property deed and information about a joint bank account.

HRDC's disclosure to the OCRT does not offend the *Privacy Act* – it was in accordance with a regulation that authorized the disclosure under an Act of Parliament. Furthermore, the OCRT is not subject to the *Privacy Act*. Nevertheless, I was concerned that the OCRT obtained more information from HRDC than was absolutely required. Some information, such as the common-law wife's SIN and details about her bank account, was not necessarily a factor in HRDC's decision, and did not need to be shared with the OCRT for appeal purposes. In response to my concerns, HRDC agreed to review the documents it intends to submit to the OCRT on a case-by-case basis, keeping in mind the privacy rights of all individuals concerned while providing sufficient information to ensure a fair and complete hearing.

Canada Post changes stance on using negative consent to sell addresses to mass mailers

My Office received a complaint that Canada Post, a Crown corporation, was improperly disclosing personal information collected for its National Change of Address (NCOA) service. The complainant stated that Canada Post was selling subscribers' new addresses to mass mailers and direct-marketing companies unless subscribers to the service contacted the corporation in writing to specifically request that their information not be used for that purpose. This practice is what is known as "negative consent," and it is something Canadians have been known to get very upset about.

For this service, individuals pay a fee to Canada Post to have their mail forwarded until they have had an opportunity to notify others of their change of address. To subscribe, they sign a Change of Address Notification (COAN) form containing the following acknowledgement:

> … I understand the information I provide will be used to deliver mail to my new address. I also agree Canada Post may supply this new address to mailers, provided they request it and already have my correct name(s) and old address.

By signing this statement, individuals asked Canada Post to perform the specific service they paid for – redirecting their mail to their new address. But they were also agreeing to something that they didn't specifically request – allowing Canada Post to sell their new address to mass mailers and direct-marketing companies – unless, as indicated on the back of the form, they wrote in and told the corporation not to do so within seven days.

Many individuals may have read this section, without realizing that "supply" meant sell and that "mailers" meant *any* mailers – primarily, companies that send junk mail.

I informed Canada Post of my concern that subscribers were not aware they were consenting to the provision of their information to mass mailers when they signed the COAN form. Canada Post argued that subscribers provided consent when they signed the form and that they could notify the corporation if they did not want their new address provided to all mailers. I pointed out that, to stop Canada Post from selling their information to mass mailers, subscribers would have to read the fine print on the front of the form that referred them to further details on the reverse side. The reverse side stated the following: "At no additional cost, Canada Post will help you advise businesses and other organizations of your new permanent address."

I disagreed with Canada Post's stance that it had obtained consent. Not only is the notion of "negative consent" insensitive to the privacy rights of Canadians, but Canada Post didn't really obtain proper consent at all. Under the *Privacy Act*, an organization does not have your consent if it has not told you what you are consenting to.

Informed consent was the real issue. Section 5(2) of the *Act* requires a Government institution to inform you of its purposes when it collects personal information from you. Was Canada Post informing those who subscribed to the NCOA service of its purposes, plainly and fully? Would reasonable persons, on reading the COAN form, conclude that they were giving consent for the sale of their personal information to mass mailers and direct marketers? I was quite sure they would not. In matters involving consent, the reasonable expectations of the individual are also relevant.

Canada Post initially agreed to adopt some of my recommendations to make the NCOA service more transparent and sensitive to privacy rights. It agreed to replace the word "acknowledgment" with "authorization" on the front of the COAN form and to add the phrase "including direct mailers" in the statement. But Canada Post was reluctant to accept my main recommendation: to give subscribers to the service a positive choice in the matter by adding an opt-in box on the front of the form. It believed that such an addition risked undermining the NCOA service and would lead to frustration and inconvenience for its customers.

I convinced Canada Post otherwise. I argued that Canada Post would benefit from such an addition, since its customers would appreciate that the corporation was doing everything in its power to maintain their privacy, and that customers would also benefit. Customers who want to receive mail from mass mailers can clearly indicate their choice, while those who don't want the junk mail will also have a choice in the matter. But the customer would have the choice, not Canada Post.

Canada Post finally agreed to add an opt-in box on its COAN form.

Incidents under the *Privacy Act*

The Investigations Branch staff makes inquiries about incidents that have come to my attention from various sources, but are not considered to be formal complaints under the *Privacy Act*. Many of these incidents concern the management (or mismanagement) of personal information – inadvertent disclosures to third parties, or lost or stolen files and electronic notebooks. Some examples follow.

Improper disclosure of SIN on Canada Child Tax Benefit forms

In one case, a newspaper reported that the Canada Customs and Revenue Agency (CCRA) had accidentally released information about individuals in western Canada in receipt of a Canada Child Tax Benefit (CCTB). When we looked into the matter, we learned that some taxpayers received page one and two of their own Notice of Determination form and page three containing information about another taxpayer. The information on page three displayed the taxpayer's Social Insurance Number (SIN), first name of the spouse where applicable, and the payment schedule for the year.

Even though the taxpayer's name is not displayed, the Social Insurance Number is a unique number assigned to that taxpayer and therefore constitutes personal information as defined by the *Privacy Act*. Fortunately, and contrary to the media report, the information did not include the other taxpayer's surname, home address, children's names or their dates of birth, or family income. Nevertheless, we've all heard stories about the results of SINs getting into the wrong hands and the havoc that this can wreak on a person's life.

CCRA also conducted its own investigation and determined that the problem was the result of a printing synchronization error, probably because of a computer glitch. To prevent a similar problem from occurring in the future, CCRA has enhanced its systems to detect any malfunction of the printer's sorting function and shut it down. Operator intervention will be required to continue the print job after appropriate inspection has been carried out. As a result of this incident, CCRA has decided that it is no longer necessary to print the Social Insurance Number on the second and any subsequent pages of the CCTB Notice of Determination form.

Gun registry documents found in dumpster

Several days before Christmas, a man called my Office to report that he had found three bags containing personal information belonging to the Canadian Firearms Program in a dumpster in a locked compound owned by the private company where he worked.

My investigators went to the scene immediately. The location was not anywhere near the Canadian Firearms Program processing site, and the dumpster was strictly used for wood products. My investigators retrieved a number of envelopes addressed to the Canadian Firearms Program, most of which contained names and return addresses of individuals.

My investigators then confirmed that, during the fall, the Canadian Firearms Program had sent packages containing personalized applications to all firearms owners, along with return envelopes pre-addressed to the Canadian Firearms Program. The information they found in the dumpster contained the pre-addressed envelopes that had been returned to the Canadian Firearms Program.

Having established that the information originated from the Canadian Firearms Program, my investigators tried to determine how it had ended up in the compound of a private company. They confirmed that the dumpster was rented by a waste management company and had been in the compound since early December.

My investigators observed that the bags found in the dumpster were covered in snow and were stuck to the bottom of the dumpster. It is likely that when the waste company retrieved the dumpster from a previous location and emptied it, the bags stayed within.

My officials contacted the Department of Justice, the Government institution responsible for the gun registration program. Officials stated that the department had contracted out the processing of the registration forms to a private company. The company is fully cognizant of the provisions of the *Privacy Act* and thought it had taken every precaution to safeguard individuals' privacy rights. However, company officials confirmed that the normal practice was to throw out the pre-addressed return envelopes using a regular garbage can, without realizing that firearms owners had written their names and return addresses on the envelopes, which would make them easily identifiable as firearms owners. The company agreed to immediately stop throwing the envelopes into the regular garbage and undertook to dispose of them in a secure manner, through shredding.

HRDC/CCRA to share data on eligibility for Guaranteed Income Supplement

I took a special interest in another situation that received a great deal of media attention – the apparent inability of the Canada Customs and Revenue Agency (CCRA) to share information with Human Resources Development Canada (HRDC) that would identify senior citizens who are eligible to receive the Guaranteed Income Supplement (GIS). The GIS is a component of the Old Age Security (OAS) benefit and is granted to those seniors in the lower income bracket. Approximately 1.5 million seniors receive the GIS. Although this case did not directly involve the *Privacy Act*, I did not want privacy legislation or my Office to be seen as a barrier preventing federal Government departments from engaging in activities that benefit Canadians.

CCRA has taxpayer information that would reveal which seniors would qualify to receive the supplement, but it refused to share their identities with HRDC's Income Security Programs Branch that grants the benefit because of the confidentiality provisions of the *Income Tax Act*. In my view, the *Income Tax Act* contains specific authorization to disclose personal information for the purpose of administering the *Old Age Security Act*, as I testified before a House of Commons committee on the matter.

Following media reports about the lack of cooperation between the two arms of Government, my Office met with officials of HRDC and CCRA to facilitate a solution to the problem, and to help ensure that seniors who qualify for the GIS are made aware of the availability of the income supplement. As a result of these efforts:

- CCRA added a page for lower income seniors to its 2001 tax guide with key messages about the GIS and how to apply;
- CCRA will send information about OAS and GIS benefits to people over age 65 who have a low or modest income; and
- HRDC will receive from CCRA a list of low-income seniors who receive the OAS benefit but not the GIS. Using income data supplied by CCRA and existing personal data from the OAS application form, HRDC will provide potential GIS clients with a simplified GIS application form containing their pre-printed name, address and income information. It will ask them to confirm or correct the information on the form so that their eligibility for GIS benefits can be decided upon return of the form to HRDC.

I understand that both HRDC and CCRA recognize the need for a more streamlined process that ensures the legal underpinnings are in place to make seniors aware of their entitlement to benefits. My staff and I are available to both departments to discuss other initiatives and to provide whatever assistance we can to ensure that there are no adverse implications from a privacy perspective.

Public Interest Disclosures

Paragraph 8(2)(m) of the *Privacy Act* allows the head of a Government institution to disclose personal information in the public interest, without the individual's express consent – either because disclosure clearly outweighs any consequential invasion of

privacy that might result, or because it would benefit the individual to whom the information relates. This provision is designed to deal with those situations where the Government institution cannot satisfy any other provision set out in subsection 8(2) of the *Act* to justify the disclosure. Subsection 8(5) of the *Act* imposes a mandatory duty on the heads of Government institutions to notify the Privacy Commissioner in writing of any public interest disclosure of personal information. The notice is to be issued in advance unless the situation requiring disclosure is so urgent and pressing that failure to act immediately would itself contribute to some identifiable harm.

This past year, I reviewed 57 notifications that personal information would be disclosed in the public interest. Almost one half of these were generated by Correctional Service Canada (CSC). CSC receives requests from third parties, including victims groups, for Board of Inquiry reports dealing with issues that have often received wide media attention, including prison escapes and violent criminal activities of offenders still under CSC supervision. It also receives requests for information from family members of offenders who died while under CSC supervision. The public interest disclosure provision of the *Privacy Act* is CSC's only authority to release personal information to the family on compassionate grounds, so that the family can have a better understanding of what happened and to help them achieve some degree of closure.

I also reviewed the circumstances related to a notification to me from the RCMP that it intended to release personal information about a convicted criminal to the media. The information requested by the media related to a videotape that had been entered into evidence in the offender's trial, which the media had wanted to use in an exposé about the criminal's highly publicized case. The media had turned to the RCMP for assistance after discovering that the Court had destroyed its copy of the tape – the Court does not retain indefinitely all evidence or exhibits presented during proceedings. The only existing copy was in the possession of the RCMP.

I failed to see how the public interest would be served by disclosing the information under these circumstances and asked the RCMP to reconsider its position. Although the tape was used as evidence in a criminal proceeding, which is public in nature, it is first and foremost personal information about an identifiable individual contained in the RCMP's investigative records, which are not generally publicly available. I therefore recommended to the RCMP that it refuse to disclose the tape. The RCMP complied with my recommendation.

Top Ten Departments by Complaints Received

April 1, 2001 to March 31, 2002

Organization	Total	Access to Personal Information	Time	Privacy	Other
Canada Customs and Revenue Agency	307	152	85	69	1
Correctional Service Canada	265	84	125	56	0
Human Resources Development Canada	117	42	57	18	0
Citizenship and Immigration Canada	103	57	40	6	0
Royal Canadian Mounted Police	89	65	16	8	0
National Defence	78	31	35	11	1
Immigration and Refugee Board of Canada	41	6	29	6	0
Canada Post Corporation	32	12	6	14	0
Justice Canada	22	6	5	11	0
Canadian Security Intelligence Service	18	18	0	0	0
Others	141	67	30	44	0
Total	**1,213**	**540**	**428**	**243**	**2**

Completed Investigations and Results by Department

April 1, 2001 to March 31, 2002

Organization	Well-founded	Well-founded/ Resolved	Not Well-founded	Discontinued	Resolved	Settled	Total
Agriculture and Agri-Food Canada	0	0	1	1	0	0	2
Atlantic Canada Opportunities Agency	0	0	0	0	0	2	2
Bank of Canada	0	0	0	0	0	3	3
Canada Customs and Revenue Agency	44	20	120	8	10	63	265
Canada Mortgage and Housing Corporation	1	0	0	0	0	0	1
Canada Post Corporation	5	7	10	2	2	16	42
Canadian Environmental Assessment Agency	0	0	2	0	0	0	2
Canadian Grain Commission	0	1	0	0	0	2	3
Canadian Heritage	0	0	1	0	0	1	2
Canadian Human Rights Commission	0	0	2	0	0	1	3
Canadian Museum of Civilization Corporation	1	0	0	0	0	0	1
Canadian Nuclear Safety Commission	0	0	0	0	0	3	3
Canadian Radio-Television and Telecommunications Commission	0	0	1	0	0	1	2
Canadian Security Intelligence Service	0	0	35	1	0	1	37
Canadian Space Agency	3	1	1	1	0	0	6
Citizenship and Immigration Canada	40	4	26	11	0	17	98

Completed Investigations and Results by Department (Continued)

April 1, 2001 to March 31, 2002

Organization	Well-founded	Well-founded/ Resolved	Not Well-founded	Discontinued	Resolved	Settled	Total
Commission for Public Complaints against the RCMP	1	2	4	0	0	1	8
Correctional Investigator Canada	1	0	0	0	0	0	1
Correctional Service Canada	344	11	47	17	1	89	509
Environment Canada	2	0	1	0	0	1	4
Farm Credit Canada	0	3	1	0	0	1	5
Fisheries and Oceans Canada	0	0	1	0	0	0	1
Foreign Affairs and International Trade Canada	24	0	4	0	0	1	29
Health Canada	0	0	0	2	0	4	6
Human Resources Development Canada	86	10	45	24	2	36	203
Immigration and Refugee Board	29	1	3	0	0	6	39
Indian and Northern Affairs Canada	1	1	9	1	1	0	13
Industry Canada	1	0	4	1	1	2	9
Justice Canada	8	1	12	4	1	8	34
National Archives of Canada	1	0	3	1	0	5	10
National Defence	44	14	20	8	3	25	114
National Gallery of Canada	0	0	0	0	0	1	1
National Parole Board	0	3	9	3	0	5	20
Natural Resources Canada	0	0	1	0	0	1	2
Office of the Chief Electoral Officer	0	1	1	0	1	2	5

Completed Investigations and Results by Department (Continued)

April 1, 2001 to March 31, 2002

Organization	Well-founded	Well-founded/ Resolved	Not Well-founded	Discontinued	Resolved	Settled	Total
Office of the Commissioner of Official Languages	0	0	0	1	0	0	1
Office of the Superintendent of Financial Institutions	0	0	1	0	0	0	1
Ombudsman National Defence and Canadian Forces	1	0	1	0	0	0	2
Privy Council Office	3	1	0	0	0	0	4
Public Service Commission of Canada	1	2	0	0	0	2	5
Public Service Staff Relations Board	0	0	1	0	0	0	1
Public Works and Government Services Canada	1	0	1	2	0	6	10
Royal Canadian Mounted Police	20	6	66	10	3	36	141
Solicitor General Canada	2	0	2	0	0	0	4
Statistics Canada	3	0	2	0	0	0	5
Status of Women Canada	0	0	2	0	0	0	2
Toronto Port Authority	1	0	0	0	0	0	1
Transport Canada	0	2	1	0	0	0	3
Treasury Board of Canada Secretariat	0	0	3	0	0	0	3
Veterans Affairs Canada	0	0	1	1	1	1	4
Western Economic Diversification Canada	0	0	0	0	0	1	1
Total	**668**	**91**	**445**	**99**	**26**	**344**	**1,673**

Completed Investigations by Grounds and Results

April 1, 2001 to March 31, 2002

	Well-founded	Well-founded/ Resolved	Not Well-founded	Discontinued	Resolved	Settled	Total
Access to Personal Information	**22**	**80**	**260**	**60**	**22**	**259**	**703**
Access	22	77	249	53	22	248	671
Correction/Notation	0	3	9	4	0	4	20
Language	0	0	1	3	0	4	8
Inappropriate Fees	0	0	1	0	0	3	4
Privacy	**184**	**11**	**99**	**26**	**4**	**73**	**397**
Collection	10	2	26	2	0	19	59
Retention and Disposal	10	2	5	1	1	7	26
Use and Disclosure	164	7	68	23	3	47	312
Time Limits	**462**	**0**	**85**	**13**	**0**	**11**	**571**
Correction/Time	4	0	0	1	0	1	6
Time Limits	440	0	53	9	0	9	511
Extension Notice	18	0	32	3	0	1	54
Other	**0**	**0**	**1**	**0**	**0**	**1**	**2**
Total	**668**	**91**	**445**	**99**	**26**	**344**	**1,673**

Origin of Completed Investigations

April 1, 2001 to March 31, 2002

Province/Territory	Number
Newfoundland	3
Prince Edward Island	4
Nova Scotia	57
New Brunswick	60
Quebec	257
National Capital Region–Quebec	11
National Capital Region–Ontario	116
Ontario	433
Manitoba	92
Saskatchewan	39
Alberta	271
British Columbia	315
Nunavut	0
Northwest Territories	0
Yukon	5
International	10
Total	**1,673**

Privacy Practices and Reviews

Introduction

Section 37 of the *Privacy Act* permits me to initiate compliance reviews, at random, of the personal information-handling practices of federal institutions. What this means is that I audit them, to verify whether they are complying with the principles for the collection, use, disclosure, protection, retention and disposal of personal information set out in sections 4 to 8 of the *Act*.

The Office has been conducting compliance reviews under section 37 since 1984. I have expanded this function during the past year, setting up a Privacy Practices and Reviews Branch, to allow me to assess how well organizations are complying with the requirements set out in the *Privacy Act* and the *Personal Information Protection and Electronic Documents Act*. (The private sector legislation gives me similar powers of audit; my discussion of private sector audit activity is in Part Two of this Report.)

As an ombudsman, I want privacy audits to be non-confrontational whenever possible. An audit, ideally, is a co-operative, constructive approach to dealing with issues before they become complaints. It's useful for organizations that want to improve their personal information-handling practices. Although I have the same powers with respect to audits that I do in investigations – to summon witnesses, administer oaths, and compel organizations to produce evidence – I would only resort to them if I didn't get voluntary co-operation.

My staff in the Privacy Practices and Reviews Branch, in addition to auditing and reviewing, works with federal organizations that are looking for a better understanding of compliance issues and the privacy implications of programs and practices. It's critical for Government departments to fully explore how privacy can be protected before they go ahead with plans, however well intentioned, to cut costs or protect citizens. On request, my branch staff reviews new proposals for information management, such as data-matching initiatives, the creation of databases and information-sharing arrangements with other organizations. This is another way to help ensure that Canadians' privacy rights are respected.

In the past year, my Office completed reviews of the personal information-handling practices under section 37 of the *Privacy Act* at the Canadian Nuclear Safety Commission (CNSC) and the Immigration and Refugee Board (IRB).

The objectives of the reviews were: to learn where and how the CNSC and the IRB handle personal information; to determine the degree to which their personal information management policies and practices are in compliance with sections 4 to 8 of the *Privacy*

Act in terms of the principles of fair information practices; and to offer observations and recommendations, where necessary. At the end of each review, organizations received reports complete with detailed findings and recommendations. I have recently issued the reports of our compliance reviews to the CNSC and the IRB, and I am awaiting their responses to the findings and recommendations.

It is not my intention to routinely disclose review findings unless the issues uncovered are so outstanding as to warrant public disclosure. An outstanding issue presented itself in the review of the IRB.

The review revealed that the Montreal, Vancouver and Toronto regional offices use closed circuit television equipment to monitor public reception and waiting rooms, as well as in hallways adjacent to hearing rooms. In some cases, video and audio equipment was installed inside hearing rooms. At the time of the compliance review, IRB did not have internal written policies or procedures regarding the use of electronic surveillance equipment, and no signage existed to inform individuals that they may be under surveillance in the areas where such devices are used.

My Office was particularly concerned about the existence of secret microphones in hearing rooms at the Montreal regional office of which headquarters were unaware. The conduct of covert surveillance – whether it involves the use of video surveillance equipment or other recording devices – is a major infringement of an individual's right to privacy and must be properly justified. No reasonable justification was provided concerning the installation of such equipment. IRB officials have since confirmed that the microphones in question have been dismantled and they assert that the listening devices were never used. My Office was also informed that the unions have been advised of the matter and that the IRB has developed a security policy requiring all regions to submit their security plans to headquarters for approval before implementation.

Update on Canadian Firearms Program

Since the mid-1990s my Office has taken a keen interest in the Canadian Firearms Program. The *Firearms Act* is a highly controversial piece of legislation that continues to produce strong emotions among both its supporters and its critics. My continued interest in the implementation of this legislation is simple: the Firearms Program involves the collection and use of a large amount of highly sensitive personal information. This legislation also has a direct impact on more than 2.3 million firearm owners, involving more than 7 million firearms in Canada. I also continue to receive complaints and inquiries about various aspects of the program, including some from Members of Parliament.

On August 29, 2001, I issued my report entitled *Review of the Personal Information Handling Practices of the Canadian Firearms Program* to the Department of Justice and the RCMP. Part 1 of the report summarized my Office's review of the program's compliance with sections 4 to 8 of the *Privacy Act* dealing with the handling of personal information. Part 2 contained our assessment of the pertinence of questions about personal history used on the firearms licence applications and their compliance with the *Privacy Act*. The report contained some 34 detailed recommendations for corrective measures aimed at reducing the intrusiveness of the program.

None of my recommendations to the Department of Justice has yet been accepted. The RCMP, however, has agreed to implement some of the recommendations from my report. I am pleased to note, for instance, that firearms officers across Canada no longer have full query access privileges to the RCMP's Police Information Retrieval System (PIRS) and that all of my recommendations with respect to limiting the use of PIRS have been implemented. In addition, I expect that the RCMP will complete the necessary revisions to the Memoranda of Understanding regarding four informatics and security areas related to the Firearms Program in the near future. These important steps will help to tighten up the control of access to sensitive personal information used in the program.

While I do not have the power under the *Privacy Act* to force the department to implement my recommendations, I will continue my efforts to urge the department to take appropriate measures to bring the Canadian Firearms Program into full compliance with the *Act*.

Subsequent to the research and fieldwork that formed the basis of my original report, other issues came to light. My Office has been monitoring the following outstanding issues:

- Outsourcing – Implementation of the existing contractual arrangement with BDP Business Data Services Ltd., all aspects of the Alternative Service Delivery initiative, as well as the current practice of outsourcing secondary and tertiary screening functions; and
- Any international information-sharing arrangements relating to the Canadian Firearms Program, whether directly or indirectly through other enforcement agencies.

Update on HRDC Governance protocol for the Databank Review Committee

In last year's Annual Report, I described how, under mounting public pressure, Human Resources Development Canada (HRDC) made the decision to dismantle the Longitudinal Labour Force File and implement a review process and a governance protocol for all policy analysis, research and evaluation activities involving the connection of separate databanks. As I explained then, this review process would involve consultation with my Office to examine such projects.

Since the last reporting period, my Office has provided comments on an additional 17 HRDC submissions, including the Review of the Action Centre for Employment, the Non-Experimental Evaluation of Investigation and Control, and the Testing of Probabilistic Record Linkage projects, to name a few. I thought it appropriate to discuss some examples of the work that we have done over the course of the year in terms of reviewing and providing comments in relation to these submissions.

My Office developed a customized assessment tool to provide a timely review of the HRDC submissions. The tool is intended to ensure that the review of such projects is consistently thorough and that all the principles of fair information practices in the *Privacy Act* are respected in the submissions. Although we are still testing its efficacy, my Office has had positive results using the tool to date.

By reviewing the development of HRDC's research projects, my Office's involvement serves as a critical check to protect privacy and often raises broader questions in relation to the use of personal information for purposes related to research and evaluation.

For instance, the Non-Experimental Evaluation of Investigation and Control (I&C) program sought to identify savings and determine the extent of deterrence resulting from I&C activities as a way of evaluating the short-term impact of the I&C function and better managing the branch. To accomplish this, HRDC research officers linked EI claim data with I&C case files and, using specific statistical methods, estimated the likelihood of EI fraud based on basic characteristics such as demographics, industry and other variables. Based on this analysis, HRDC researchers produced an equation that could be used to estimate the likelihood of EI fraud for other EI claims and therefore to evaluate the effectiveness of I&C interventions.

Although the objectives of the evaluation project were detailed and HRDC had the authority to evaluate the program, the submission was unclear with respect to the subsequent use of this equation following completion of the evaluation project. My

Office was concerned that, although it was created in the context of research, HRDC could eventually use such an equation to make decisions directly affecting individuals, such as by systematically profiling all EI claims for potential investigations solely based on the results of the equation. Since access to the personal information was strictly for research and evaluation purposes, my Office was of the view that I&C could not use the equation for administrative or enforcement purposes directly affecting a particular individual.

My Office clarified this issue with HRDC, which confirmed that it never intended to use the equation for operational purposes and, specifically, that it would not use the method to profile individuals for investigation. HRDC effectively established a clear separation between its research work and its enforcement branch. Although it is clear that HRDC had implemented the appropriate practices in relation to this project, the example serves to illustrate that use of personal information for "research or evaluation purposes" can have potential pitfalls if left unchecked.

It is worth noting that my Office has noticed a marked improvement in the level of detail and completeness of HRDC's project submissions in terms of addressing privacy concerns. Nevertheless, there is always room for improvement when it comes to privacy. In reviewing some of the HRDC submissions a common deficiency was noted: since many of the proposals are not yet finalized, they only provide limited information in relation to contracts involving outside parties.

Although HRDC has provided some examples of proposed contractual language, there is often little or no reference to the *Privacy Act*. My Office has insisted on the importance of protecting privacy in contractual agreements with consultants and third parties. We have clearly stipulated that all such contractual agreements must state that all personal information involved in the research is deemed to be under the control of HRDC; that such information is subject to the provisions of the *Privacy Act*; and that consultants and third parties must explicitly undertake to comply with all of the requirements of the *Act*.

The significance of this clause is two-fold. First, it holds the consultant accountable to the same standards of information management that are in place across Government and, second, it ensures that the provisions related to the conduct of reviews and investigations contained in the *Privacy Act* are applicable and enforceable. Although we have every confidence that HRDC is integrating these clauses in its contracts, it is important to remember that part of my role is to conduct reviews to determine whether the actual privacy practices of a Government organization are consistent with the fair information principles under the *Privacy Act*.

In the Courts

Introduction

Section 41 of the *Privacy Act* allows an individual, following my investigation, to apply to the Federal Court of Canada for review of a Government institution's decision to refuse the individual access to his or her personal information. From the time the *Privacy Act* came into force in 1983, 118 applications for review have been filed in the Federal Court. Twelve of these were filed in the year ending March 31, 2002.

Section 42 of the *Privacy Act* allows me to appear in Federal Court. I can apply to the Federal Court for review of a Government institution's decision to refuse access to personal information if I have the consent of the individual who requested the information; appear before the Court on behalf of an individual who has applied for review under section 41; or, with leave of the Court, appear as a party to any review applied for under section 41.

The following is not an exhaustive list of all *Privacy Act* applications in the courts but rather a summary of matters in which I am actively involved:

Traveller Declaration Forms (Form E-311)

We pursued two cases based on the disclosure of personal information by Canada Customs and Revenue Agency (CCRA) to the Canada Employment Insurance Commission (CEIC) for use in an investigative data match program to determine if persons were fraudulently receiving Employment Insurance benefits while outside of Canada. The personal information in question was taken from Traveller Declaration Forms (E-311 forms) presented to Customs by Canadian residents returning to Canada between 1994 and 1996.

- *Privacy Commissioner v. Attorney General of Canada*
  The Federal Court of Appeal found that the disclosure of personal information from the E-311 forms was authorized by section 8(2)(b) of the *Privacy Act* and section 108 of the *Customs Act*, which gave the Minister of National Revenue discretion to disclose information collected by the department. In this case, the Court found the disclosure of information by the CCRA to the CEIC pursuant to an MOU governing terms and conditions of disclosure to be authorized. (Section 108 of the *Customs Act* has now been amended under Bill S-23.)

- *The Charter Challenge*
  The Federal Court of Appeal found there to be no reasonable expectation of privacy sufficient to engage section 8 of the *Canadian Charter of Rights and Freedoms* in the information contained in E-311 forms. This conclusion was based on two elements: the limited nature of the information in question, which did not reveal intimate details of the lifestyle and personal choices of the individual, and the narrow enforcement use to which the information was put.

Status

The cases were heard on November 7, 2001. The Supreme Court of Canada released its decisions in both cases on December 7, 2001. In each case, the reasoning of the Federal Court of Appeal was affirmed. In the Charter Challenge, the Supreme Court specifically concluded that there was no reasonable expectation of privacy in relation to the disclosed portion of the E-311 information which outweighed the CEIC's interest in ensuring compliance with the self-reporting obligations of the Unemployment Insurance benefit program.

Information Commissioner of Canada v. Commissioner of the RCMP and Privacy Commissioner

A list of the career postings of four named Royal Canadian Mounted Police (RCMP) officers was requested under the *Access to Information Act*. The Commissioner of the RCMP refused to release the information on grounds that it revealed employment history and thus was personal information as defined in section 3 of the *Privacy Act*.

At issue was whether the information could be disclosed under paragraph (j) of the definition of personal information in the *Privacy Act*, which states that information relating to the position or functions of Government officers or employees is not personal information. The larger question was the appropriate balance between the provisions of the *Access to Information Act* and those of the *Privacy Act*. The Federal Court of Appeal held that the information was personal information and did not fall under the paragraph (j) exception. The Court found that the exception should be construed in a way that does not allow for the disclosure of an individual's employment history.

Status

The Information Commissioner obtained leave to appeal this decision to the Supreme Court of Canada. I was granted leave to intervene in the appeal on January 7, 2002. The case was heard on October 29, 2002, after which the Court reserved its decision.

Clayton Charles Ruby v. Solicitor General

The Canadian Security Intelligence Service (CSIS) refused Mr. Ruby's request for access to his personal information. Mr. Ruby filed for a court review under section 41 of the *Privacy Act*.

During the court review, Mr. Ruby raised *Charter* concerns regarding the constitutionality of section 51 of the *Privacy Act*. This section provides for closed hearings (in camera) or hearings that exclude one party to the conflict (*ex parte*), where a Government institution has claimed the "foreign confidences" or the "national security" exemptions under the *Act*. The Federal Court of Appeal decided that these provisions (sections 51(2)(a) and 51(3) of the *Privacy Act* respectively) infringed on the freedom of the press, which is protected by section 2(b) of the *Charter*, but those provisions were justified under section 1 of the *Charter*. The provisions were found not to violate the right to life, liberty and security of the person protected by section 7 of the *Charter*.

Status

Mr. Ruby was granted leave to appeal to the Supreme Court of Canada concerning the *Charter* issue on January 18, 2001. The Solicitor General was granted leave to cross-appeal, and I was granted leave to intervene, on an issue concerning the interpretation of section 22(1)(b) of the *Privacy Act*. The case was heard by the Supreme Court of Canada on April 24, 2002 and the decision was rendered on November 21, 2002.

The Supreme Court held that the section 51 procedures in the *Privacy Act* do not fall below the level of fairness required by section 7 of the *Charter*. The Court did not find it necessary to the disposition of the case to decide on the privacy arguments raised by Mr. Ruby under section 7. Therefore, from a privacy perspective, the ruling does not affect the status quo. The mandatory *in camera* provision in section 51 does, however, contravene section 2(b) of the *Charter*. The Supreme Court further found that the provision could not be justified under section 1 of the *Charter*. The provision is unconstitutional and must be "read down" to apply only to those parts of the hearing that involve the merits of an exemption. The Supreme Court noted that the past judicial practice under section 51 was in fact to conduct the hearing in open court and to hear only the merits of the exemptions in camera.

With respect to the cross-appeal, the Supreme Court confirmed the finding it made in *Robert Lavigne v. Office of the Commissioner of Official Languages* on the interpretation of section 22(1)(b) of the *Privacy Act* (as follows).

Robert Lavigne v. Office of the Commissioner of Official Languages

Mr. Lavigne was refused access to information about himself contained in witness statements made in the course of an investigation conducted by the Office of the Commissioner of Official Languages. The office based its refusal of access on the exemption contained in section 22(1)(b) of the *Privacy Act*.

The Federal Court of Appeal held that section 22(1)(b) can only be invoked where there is evidence of injury to a specific investigation; that it cannot be invoked once the specific investigation has been completed; and that the allegation of a "chilling effect" on future investigations is not sufficient to support refusal to disclose.

Status

The Commissioner of Official Languages was granted leave to appeal to the Supreme Court of Canada on April 19, 2001. I was granted leave to intervene in support of Mr. Lavigne. The case was heard by the Supreme Court of Canada on January 17, 2002 and its decision was released on June 20, 2002.

The Supreme Court concluded that the exemption in section 22(1)(b) was not limited to current investigations. However, where an institution wishes to rely on the exemption in respect of harm to future investigations, it must be able to demonstrate a clear and direct connection between the disclosure of the information and the injury that is alleged.

The Supreme Court found that the Office of the Commissioner of Official Languages had not satisfied this test and ordered that Mr. Lavigne be given access to his personal information.

Information Commissioner of Canada v. Minister of Citizenship and Immigration Canada and Philip W. Pirie

Mr. Pirie was refused access to the identities of employees who gave views or opinions about him during an administrative review conducted by Citizenship and Immigration Canada. The information was withheld as the personal information of those employees under section 19(1) of the *Access to Information Act*.

The Federal Court Trial Division concluded that the identity of the individuals who expressed views about Mr. Pirie was their own personal information and should not be disclosed to Mr. Pirie.

Status

The Information Commissioner filed an appeal arguing that the identities of individuals who commented about Mr. Pirie during the review process are the personal information of Mr. Pirie under paragraph (g) of the definition of personal information in the *Privacy Act*. I was granted leave to intervene at the Federal Court of Appeal in support of the Information Commissioner's position. The matter was heard on June 4, 2002 and the Court's decision was released on June 21, 2002.

The Federal Court of Appeal agreed with the Information Commissioner and me that the identities of the persons interviewed should be disclosed to Mr. Pirie. The Court observed that the names of the interviewees were personal to both Mr. Pirie and to the interviewees, but that one interest must prevail over the other. The Court looked at the private and public interests at stake, and concluded that both mandated the disclosure of the names to Mr. Pirie. This decision is not being appealed to the Supreme Court.

Mertie Anne Beatty et al. v. the Chief Statistician et al.

This is a recent application brought by a group of Canadian citizens who seek access to the 1906 census returns for the provinces of Manitoba, Saskatchewan and Alberta. The applicants seek an order compelling the Chief Statistician to transfer the 1906 census returns to the National Archivist, and an order directing the National Archivist to make the returns available to the public for research purposes in accordance with section 6 of the *Privacy Regulations.*

Status

The application was filed on February 5, 2002, and I was one of the named respondents. All arguments have now been filed. A hearing date has not been set.

Part Two
Report on the *Personal Information Protection and Electronic Documents Act*

Introduction

A year is not long in the life of a law – not long enough, perhaps, to afford a basis at present for a comprehensive analysis of the application of the *Personal Information Protection and Electronic Documents (PIPED) Act*. Still, from the 28 investigations we finalized under the *PIPED Act* in 2001, I was able to draw some fairly solid conclusions on two fronts at least, and I believe it is instructive to share those conclusions at this time. (I will report on the experience with the second year of the *PIPED Act* in my upcoming next Annual Report.)

In particular, there has been considerable progress made in interpreting what is and what is not personal information, and in determining areas in which organizations typically seem to be having problems adapting to the requirements of the *Act*.

The Definition of Personal Information: Broad but not Infinite

Section 2 of the *PIPED Act* defines personal information simply as "information about an identifiable individual." That definition is meant to cover a lot of ground, and the first year of the *Act* served in good measure to clarify what ground it does, and does not, cover.

Several cases have already given rise to disputes over whether the information at issue constituted the complainant's personal information. Notably, some organizations have been quick to claim "ownership" of certain items of information assigned to customers, such as account numbers, identification numbers and credit cards. The usual argument is that such information should not be considered personal because it is not collected from customers. Because it is generated internally by the organization itself, it is deemed by corporate convention to be the organization's property.

But the section 2 definition was designed to sidestep such arguments. It doesn't say that personal information has to originate with or be collected from the individual. It doesn't concern itself with who may or may not be said to have proprietary interest in the information. It only says that information is personal if it is "about" an identifiable individual. When it comes right down to it, if an organization has put someone's name on something, it is difficult for the organization to argue that the thing isn't "about" that individual.

The definition is deliberately broad, and in my findings I have tended to interpret it as broadly as possible. Generally speaking, it does not matter who generated the information, or how, or who technically "owns" it, or what the corporate convention may be. If it has been assigned in an individual's name, the chances are that I will accept it as being his or her personal information.

I am inclined to regard information as personal even if there is the smallest potential for it to be about an identifiable individual. A case in point was one in which a broadcaster had attempted – inadvertently, as it turned out – to collect NETBIOS information from the computer of a Web site visitor. Our investigation revealed that, in certain technical circumstances such as the complainant's, NETBIOS information could be used to trace the computer's Internet Protocol address, which in turn could be used to trace Web sites visited by the user or recent passwords to secure accounts. On the basis of the potential for intrusion into the complainant's privacy, I determined that the information at issue was personal information for purposes of the *PIPED Act*.

But even a deliberately broad definition must have limits. In a much-publicized case, I took the view that section 2 was not so broad as to encompass all information associated with an individual. Specifically, I determined that physicians' prescriptions or prescribing patterns did not constitute personal information about

the physicians themselves. An individual prescription, I reasoned, is potentially revealing about a patient, but it is not in any meaningful sense about the prescribing physician as an individual. Rather, it is about the professional process that led to its issuance and should therefore be regarded as a work product – that is, the tangible result of the physician's work activity.

I judged furthermore that extending the definition to include prescriptions and prescribing patterns would not be consistent with the *PIPED Act*'s purpose. Section 3 sets out that purpose in terms of balancing the individual's right of privacy with the need of organizations to collect, use or disclose personal information for purposes that a reasonable person would consider appropriate. I did not think it reasonable to extend the definition to prescriptions, since that would mean extending it also to other work products such as legal opinions or documents written in the course of employment. Nor did I think it reasonable to extend the definition to prescribing patterns, since that would mean extending it also to patterns discoverable in other types of work products and thus would preclude many kinds of legitimate consumer reporting.

Systemic Problems

Privacy code only the beginning

It is the rare organization nowadays that isn't greatly concerned about the privacy rights of individuals – on paper, at least. Most corporate brochures and Web sites proudly proclaim a privacy code, ostensibly in full compliance with corporate obligations under the *PIPED Act*. What our complaint investigations are showing, however, is that some organizations have been less than thorough about putting their codes into practice.

A privacy code is pointless without comprehensive and detailed policies and procedures, and these in turn are pointless unless they are known and consistently observed and applied. The privacy violations that give rise to complaints are often attributable to problems or defects in an organization's information-handling processes or system as a whole. Such problems are themselves often caused by failure on an organization's part to grasp, or turn its attention to, the practical implications of the *PIPED Act*'s principles. Sometimes, too, the problems derive from unquestioned adherence to traditional practices that may no longer be acceptable under the *Act*.

The following are a few of the systemic problems that our investigations have been turning up.

Not designating a privacy officer

Principle 4.1 of Schedule 1 to the *PIPED Act* states that an organization must designate one or more individuals responsible for the organization's compliance with the principles of the *Act*. In more than one case, we have found that the organization had not yet designated such an individual or did not identify any person as the responsible privacy officer.

Not knowing how to handle access requests and complaints

Most organizations seem to understand that an individual has a right to gain access to his or her personal information (Principle 4.9) and to challenge an organization's compliance (Principle 4.10). However, when it comes down to receiving an actual access request or complaint from an individual, some organizations are still uncertain how to go about processing it. At this point, it is especially important to have specific policies and procedures in place and to follow them thoroughly and consistently.

Keeping information too long or not long enough

Retention is another principle to which some organizations need to pay greater heed in the form of specific guidelines and procedures. Under Principle 4.5.2, a minimum and a maximum retention period should be established for personal information. Information that has been used to make a decision about an individual must be kept long enough to allow the individual access to the information. Under Principle 4.5.3, information no longer required to fulfil identified purposes should be destroyed, erased or made anonymous.

What we have been finding in some cases is that organizations are either destroying personal information too soon – that is, before the individual has a chance to gain access to it – or habitually keeping it for long periods of time, far past any need to do so. In one case, we learned of an organization that was in the habit of keeping the information it collected from *unsuccessful* credit card applicants for indefinite periods of time and for no particular reason. We even learned of one organization that never destroyed any of the personal information it collected, just because it didn't know it was allowed to.

Not meeting the time limit

As provided in section 8 of the *PIPED Act*, I have already determined in a number of cases that organizations have in effect refused individuals' access requests by having exceeded the 30-day time limit for response. In most of these cases, however, the failure to meet the time limit was due more to a lack of efficient procedures for processing the requests than to deliberate refusal on the organization's part.

Not limiting collection to what is necessary

Is it appropriate for an organization, such as an Internet company, to insist on having your Social Insurance Number (SIN)? The short answer is no; there are very few private sector organizations that have a legitimate reason for collecting SINs from customers (financial institutions sometimes need to collect them for revenue reporting purposes, for example).

But in one noteworthy complaint last year, collection of SINs was the central issue. In that case, it had been the company's policy for some time to collect SINs as a means of avoiding confusion over similar names among customers. The company had never really considered whether that purpose was a legitimate one, and front-line staff had come to regard the collection as a requirement. In my finding, I determined that the collection was unnecessary and indiscriminate and that it was clearly wrong of the company to require applicants to provide their SINs as a condition of service.

This was not the only case where an organization collected more information than it really needed to fulfil legitimate purposes. Under the *PIPED Act*, organizations must take pains to ensure not only that their purposes for collecting personal information are legitimate and reasonable ones, but also that both the amount and type of information collected are necessary to fulfil those purposes. Reviewing longstanding and long-unquestioned collection policies and practices is the best way for an organization to start complying with Principle 4.7, limiting collection.

Not identifying purpose for which information collected

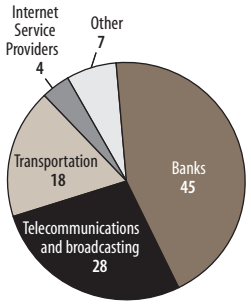
Persons from whom organizations demand information have a right to know why. It is therefore not enough that purposes be legitimate. They must also be identified.

Under Principle 4.2, an organization must identify the purposes for which it collects information. Under Principle 4.2.1, the purposes must be documented. Under Principle 4.2.3, the organization should specify the purposes to the individual at or before the time of collection. And under Principle 4.2.5, it is incumbent on the organization to make sure that employees who do the collecting can explain the purposes to individuals who question the practice.

Several complaints so far have brought to light violations of one or more of these principles. Again, in some cases the cause has been a slowness to understand that standard ways of doing things in the past are not necessarily acceptable now that the *PIPED Act* is with us.

Complaints by Sector

January 1, 2001 to December 31, 2001



Not instituting proper safeguards

In one case last year, I found that an organization's reliance on a credit cardholder's telephone number or year of birth was not adequate to prevent unauthorized access to the individual's personal information. In another case, involving loss of documents, I found that an organization had not taken proper measures to protect personal information during a transfer of files to another building. In yet another, I found that a company was not exercising appropriate operational controls in a workplace to keep employees' pay statements confidential.

In these and other cases involving actual or potential breaches of informational security, the central issue was the adequacy of the safeguards instituted by certain organizations. Principle 4.7 states that personal information must be protected by security safeguards appropriate to the sensitivity of the information. Depending on the nature of the information, safeguards may take many forms, ranging from physical measures such as locked filing cabinets, to organizational measures such as security clearances, to technological measures such as the use of passwords and encryption.

The obligation to protect personal information once it has been collected is obviously one that some organizations need to start taking more seriously.

Not recognizing that employees have privacy rights too

There is considerable evidence that some organizations that are federal works, undertakings or businesses, upon reading that the *PIPED Act* applies to the collection, use and disclosure of personal information, have jumped to the conclusion that it refers only to information about their customers. It appears not to have occurred to such organizations that, in the everyday course of business administration, they also handle a great deal of personal information about the individuals who work for them.

As a result, some organizations have been taken off guard by certain well-founded complaints against them under the *PIPED Act* – complaints filed by their own employees, past or present. In good part, the violations at issue in such complaints originate in an organization's neglect to take its staff into account in developing privacy policies and procedures.

Positive Responses to my Recommendations

Despite the foregoing, I find it encouraging that, once systemic problems have been pointed out to them, organizations by and large have been quick to accept and implement the remedies that I have recommended.

Overall, I am pleased with the progress of the *PIPED Act* so far, and with the efforts that organizations are making to bring themselves into compliance with it.

Definitions of Findings under the *PIPED Act*

Not well-founded: This means that there is no evidence to lead the Privacy Commissioner to conclude that the organization violated the *Personal Information Protection and Electronic Documents (PIPED) Act.*

Well-founded: This means that the investigation revealed that the organization failed to respect a provision of the *PIPED Act.*

Resolved: This means that the organization has taken corrective action to remedy the situation, or that the complainant is satisfied with the results of the inquiries made by the Office of the Privacy Commissioner of Canada.

Discontinued: This category applies to investigations that are terminated before all the allegations have been fully investigated. A case may be discontinued for any number of reasons, for example, when the complainant is no longer interested in pursuing the matter.

Privacy Practices and Reviews

The *Personal Information Protection and Electronics Documents (PIPED) Act* allows me to audit the compliance of private organizations if I have "reasonable grounds to believe" that the organizations are contravening a provision of the *Act* or are not following a recommendation set out in Schedule 1.

The Privacy Practices and Reviews Branch of my Office will conduct compliance reviews and audits under section 18 of the *PIPED Act*, following accepted standard audit objectives and criteria. As I mentioned in my previous *Annual Report to Parliament*, I have not yet initiated any such audit because no matter has been brought to my attention that meets the reasonable grounds test.

In the Courts

Under section 14 of the *Personal Information Protection and Electronic Documents (PIPED) Act*, an individual complainant has a right, following my investigation, to apply to the Federal Court of Canada for a hearing in respect of any matter on which the complaint was made or that is referred to in the Commissioner's report. These matters must be among those in the Schedule clauses and sections of the *Act* listed in section 14. I may also apply to the Court in respect of any complaint I have initiated. From the time the *Act* came into force on January 1, 2001, five applications have been filed in the Federal Court.

Section 15 of the *PIPED Act* allows me to apply to appear in Federal Court. I may, with the consent of the complainant, apply directly to the Court for a hearing in respect of any matter covered by section 14; appear before the Court on behalf of any complainant who has applied under section 14; or, with the leave of the Court, appear as a party to any section 14 hearing.

The following is not an exhaustive list of applications in the courts but a listing of matters of particular interest.

Mathew Englander v. Telus Communications Inc.

This is the first application to be filed in the Federal Court under section 14 of the *PIPED Act*. Mr. Englander argues that Telus uses and discloses customers' names, addresses and telephone numbers in its white pages directories and otherwise, without customers' knowledge and consent, and inappropriately charges customers for choosing to have their telephone number "non-published." He claims that these actions by Telus contravene subsections 5(1) and (3) of the *Act*, as well as several clauses of Schedule 1 of the *Act*.

Status

A hearing date has not been set.

Ronald G. Maheu v. IMS Health Canada and the Privacy Commissioner of Canada

Ronald Maheu applied for a hearing in the Federal Court of Canada, arguing that IMS Health Canada improperly discloses personal information by selling data on physicians' prescribing patterns without their consent.

Status

In his application, Mr. Maheu had asked the Court to review my "decision" in this case. I filed a motion objecting to the manner in which Mr. Maheu had framed his application, arguing that under the *PIPED Act* it is the responsibility of the organization concerned (here, IMS), and not the Privacy Commissioner, to justify why it should not have to modify its practices to comply with the *Act*. On February 12, 2002 the Federal Court ordered Mr. Maheu to file an amended Notice of Application removing allegations and requested orders against my Office, and ordered that his application be directed solely against IMS Health Canada. I was also granted leave under section 15(c) of the *Act* to appear as a party respondent in support of my finding in this proceeding. On May 14, 2002, in response to a motion brought by IMS, the Federal Court ordered Mr. Maheu to post security for costs. Mr. Maheu has successfully appealed this order.

Communications and Public Education

The *PIPED Act* has given me and my Office a greater responsibility, an expanded role and a strengthened legislative mandate to educate Canadians and organizations about issues surrounding personal privacy.

To meet these new responsibilities and in preparation for the communications activities ahead, my Office's communications capabilities were expanded. Since then, we have been proactively involved in a variety of activities to raise public awareness and understanding of issues that could potentially threaten Canadians' privacy, to inform Canadians of their legislated privacy protections and to remind private sector organizations of their responsibilities under the new legislation.

In view of my mandated responsibilities under section 24 of the *Act*, I am gratified by the increased awareness of privacy rights and privacy issues that these activities appear to be generating.

Speaking engagements

Conferences and other special events, in Canada and around the world, have provided me with a unique opportunity to meet Canadians and to raise awareness of privacy issues among diverse audiences and settings – professional and industry associations, non-profit and advocacy groups, universities and public events.

From January 1, 2001 to March 31, 2002, I gave a total of 55 speeches; another 35 were delivered by other senior staff of this Office. At these events, I spoke out about issues such as workplace privacy, genetic privacy, the application of the *PIPED Act* and its implications for businesses, the Government On-Line initiative, my grave concerns regarding video surveillance by public authorities in public places, and the need to balance privacy rights with security objectives following the terrorist attacks in the United States.

At international conferences, I had the opportunity to share my perspective on the Canadian experience with officials and privacy advocates from other countries.

Media relations

The media's appetite for news relating to privacy has continued to increase steadily. Our analysis of news coverage indicates a growing interest in the issues and in awareness of this Office. The number of calls from journalists, which currently averages approximately 100 per month, continues to increase. From January 1, 2001 to March 31, 2002, I granted more than 270 interviews to reporters.

In addition to responding to the demand for more information and comment about personal privacy and Canadians' rights under federal privacy laws, my Office has taken a number of steps to raise awareness of various issues through the media. During this period, we disseminated more than 25 news releases and media advisories, participated in a number of editorial board meetings of daily newspapers across the country, contributed articles and other information to several publications, and provided media relations support for conferences, public meetings and other special events.

Public education materials

In 2001, my Office produced two guides in anticipation of a demand from Canadians and businesses for more information about the *PIPED Act*. Our *Citizens' Guide* tells Canadians about their rights under the new law. The *Business Guide* informs organizations of their responsibilities under the law, so they can learn how to comply with it.

The Office receives requests for these guides on a daily basis and the demand is increasing. Not only are these materials sent to individuals upon request, they are also distributed at conferences and accessed in electronic format by visitors to our Web site. During this period, more than 24,000 of the guides were distributed.

In addition to the *Citizens' Guide* and the *Business Guide*, this Office has produced and distributed other educational and promotional materials, including bookmarks, posters, fact sheets, annual reports and copies of both federal privacy laws.

Plans are currently underway to identify other suitable locations where the guides and the other information could be offered to Canadians.

Advertising

Advertising is another important tool my Office has used to raise public awareness and understanding of privacy issues.

In 2001, we placed advertisements in daily and community newspapers. The ads provided information on the new legislation and its application to federally regulated businesses.

In 2002, we initiated another national advertising campaign. Radio spots were produced in English and French, and were aired on the top stations in every market across the country. These radio ads emphasized Canadians' rights under the new law and my Office's role in helping to protect those rights.

Both advertising campaigns reached millions of Canadians and resulted in nearly doubling the number of inquiries to this Office.

Public inquiries

The Communications and Policy Branch also responds to thousands of inquiries from the general public who contact my Office for advice and assistance on all sorts of privacy-related matters.

Web site

In the spirit of openness and transparency, every effort is made to ensure that new and useful information is posted on my Office's Web site on an ongoing basis and in a timely manner. New elements such as speeches, news releases, fact sheets, selected reports and case summaries are always being added to keep the site current and interesting.

Over the past year, because organizations wanted a better understanding of how the *PIPED Act* was being applied, a new section entitled "Commissioner's Findings" was added to the site. Here, summaries of my findings are posted in an effort to provide guidance to businesses and the legal community.

In 2001, the Web site was redesigned and the number of visits to the Web site has increased steadily, with a surge that resulted in almost double the visitors after October 2001. Over the period, the site averaged approximately 16,000 hits per month.

Communications Activities

January 1, 2001 to March 31, 2002

Activity		Number
Speeches delivered by Privacy Commissioner		55
Speeches delivered by senior staff		35
News releases		25
Media interviews		270
Distribution of materials		**34,036**
Business Guides	14,170	
Citizens' Guides	10,666	
Other (Annual Reports, bookmarks, fact sheets, *Act*s, etc.)	9,200	
Average number of visits to Web site per month		16,079

Inquiries by type under *Privacy Act*

April 1, 2001 to March 31, 2002

Subject	Number
Adoption/genealogy	35
Access to personal information *	504
Census	297
Collection, use and disclosure *	224
Consent issues *	25
Corrections *	18
Criminal records, pardons	203
E-311 Travel Declaration Form **	26
Firearms	76
Law enforcement *	60
Medical records **	98
No jurisdiction (federal)	983
Office of the Privacy Commissioner of Canada *	111
Personal health information *	49
Privacy Act, interpretation and process	6,988
Publication requests	189
Redirect – external	3,240
Social Insurance Numbers	410
Video surveillance *	50
Workplace surveillance *	13
Calls from Members of Parliament	31
Other	642
Total	**14,272**

* These categories were compiled from January to March 2002 only.
** These categories were compiled from April to December 2001 only.

Inquiries by type under the *PIPED Act*

January 1, 2001 to December 31, 2001

Subject	Number
Criminal records	31
Drug testing	3
Encryption	7
Financial institutions	1,609
Identity theft	38
Information request	2,744
Interception/monitoring	154
PIPED Act, interpretation and process	2,151
Jurisdiction	2,103
Marketing	462
Medical records	144
Publication requests	679
Social Insurance Number	1,902
Telecommunications	827
Transportation	152
Calls from Members of Parliament	7
Other	388
Total	**13,401**

Part Three
Corporate Services

In order to manage the implementation of the *PIPED Act*, and because of an increased mandate under the *Act*, my Office has experienced an increase in resources, both human and financial.

On April 1, 2001, my Office's budget was increased to $11.1 million from $8.7 million the previous year, and will be maintained for the next fiscal year to support the following:

- An increase in communications activities, inquiries and complaints;
- An increase in the number of investigators, auditors and Privacy Impact Assessment officers to handle issues in relation to both federal privacy laws;
- An extension of our hours of operation – now from 9 a.m. to 5 p.m. in all time zones across Canada;
- The establishment of a solid management framework which incorporates both the investigative and audit functions of the Office; and
- The establishment on April 1, 2002 of a dedicated corporate services branch for this Office, for information technology, human resources, finance and administration purposes (previously, corporate services were shared with the Office of the Information Commissioner).

In preparation for the full implementation of the *PIPED Act* on January 1, 2004, a financial framework for funding will be presented to the Treasury Board Secretariat to substantiate future expenditures.

Resources

April 1, 2001 to March 31, 2002

	FTEs	Expenditure Totals	Percentage of Total
Privacy	93	$ 9,435,901	82%
Corporate Services	15	$ 2,021,867	18%
Total	**108**	**$11,457,768**	**100%**

Note: FTE stands for "full-time equivalent" or full-time staff as of March 2002.

Detailed Expenditures

April 1, 2001 to March 31, 2002

	Privacy	Corporate Services	Total
Salaries	$5,101,779	$1,078,633	$ 6,180,412
Employee Benefits Program	1,172,850	167,150	1,340,000
Transportation and Communication	446,109	132,985	579,094
Information	1,566,375	7,502	1,573,877
Professional Services	656,962	223,749	880,711
Rentals	11,412	20,923	32,335
Repairs and Maintenance	50,453	19,920	70,373
Materials and Supplies	99,053	40,494	139,547
Acquisition of Machinery and Equipment	298,673	330,147	628,820
Other Subsidies and Payments	32,235	364	32,599
Total	**$9,435,901**	**$2,021,867**	**$11,457,768**

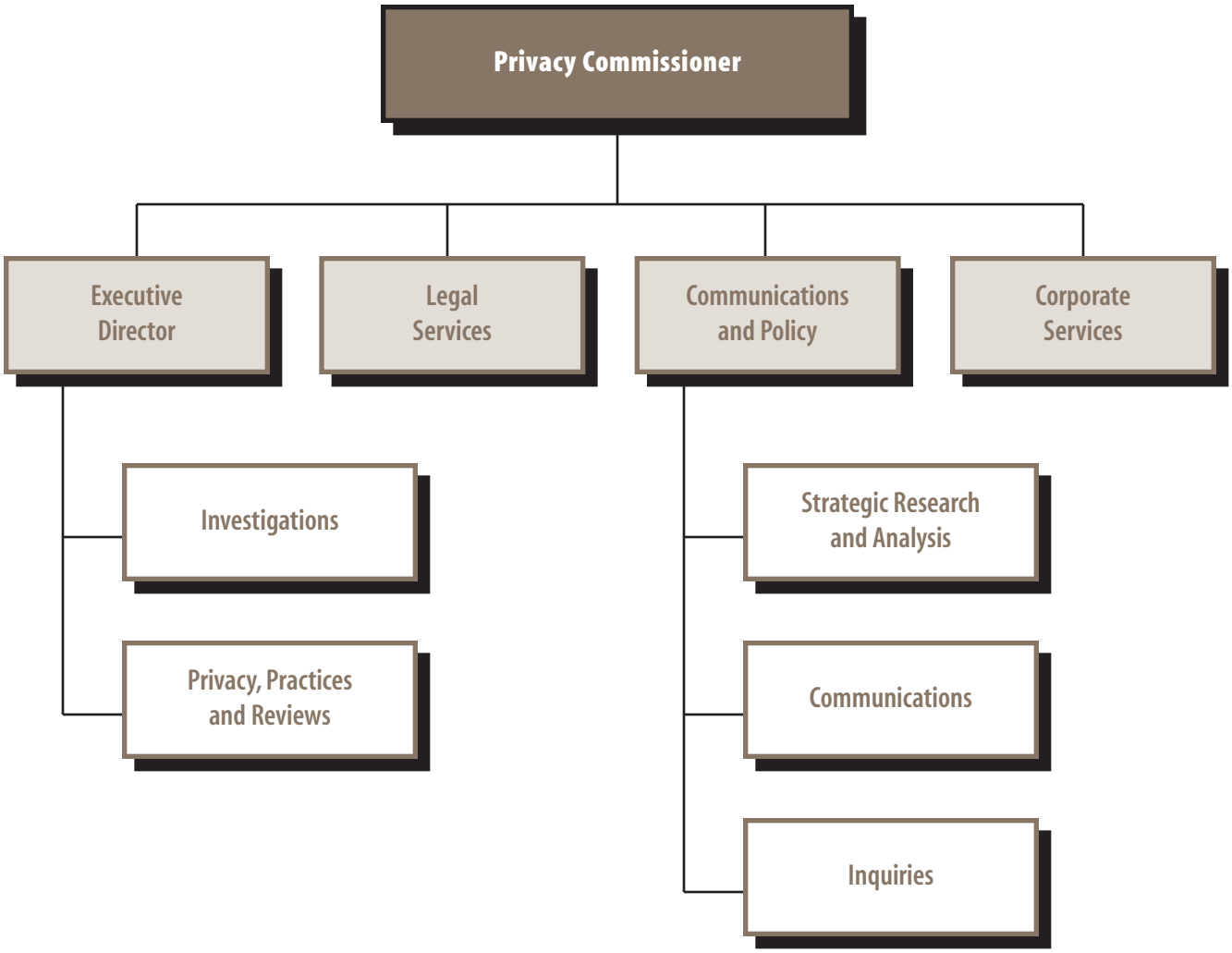
Notes:

[1] Total expenditure figures are consistent with public accounts.

[2] Expenditures for Corporate Services were allocated on a 50/50 basis and shared between the Offices of the Privacy Commissioner of Canada and the Information Commissioner of Canada.

[3] Effective April 1, 2002, Corporate Services is part of this Office and services are no longer shared with the Office of the Information Commissioner of Canada.

Corporate Structure



- Effective April 1, 2002, Corporate Services is part of this Office and resources are no longer shared with the Office of the Information Commissioner of Canada.