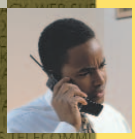
The Privacy Commissioner of Canada

Commissaire à la protection de la vie privée du Canada

Annual Report to Parliament 2000-2001



The Privacy Commissioner of Canada

Commissaire à la protection de la vie privée du Canada

Annual Report to Parliament 2000-2001

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. IP30-1/2001
ISBN 0-662-66226-1

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

December 2001

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, 2000 to March 31, 2001, for the *Privacy Act* and from January 1, 2001 to November 30, 2001, for the *Personal Information Protection and Electronic Documents Act.*

The timing of this year's report is exceptional. I had decided to submit the report in early autumn this year rather than in the spring as usual, for two reasons: first, having taken up my position in September 2000, I wanted a sufficient time frame of experience on which to report; and, second, with the *Personal Information Protection and Electronic Documents Act* having come into effect on January 1, 2001, I wanted the report to encompass a reasonable amount of experience with the new legislation. Then the events of September 11, and the privacy issues arising from their aftermath, necessitated waiting until now. The normal reporting schedule of my Office will be resumed with a report next spring.

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

December 2001

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, 2000 to March 31, 2001, for the *Privacy Act* and from January 1, 2001 to November 30, 2001, for the *Personal Information Protection and Electronic Documents Act.*

The timing of this year's report is exceptional. I had decided to submit the report in early autumn this year rather than in the spring as usual, for two reasons: first, having taken up my position in September 2000, I wanted a sufficient time frame of experience on which to report; and, second, with the *Personal Information Protection and Electronic Documents Act* having come into effect on January 1, 2001, I wanted the report to encompass a reasonable amount of experience with the new legislation. Then the events of September 11, and the privacy issues arising from their aftermath, necessitated waiting until now. The normal reporting schedule of my Office will be resumed with a report next spring.

Yours sincerely,

George Radwanski
Privacy Commissioner of Canada

Table of Contents

Commissioner's Overview

George Radwanski
Privacy Commissioner of Canada

This is my first report to Canadians as Privacy Commissioner. It's a welcome opportunity to look back and take stock of the past year. In just that short time, we've seen extraordinary developments, both technological and social, with unprecedented impacts on privacy. And for me personally, it's been a remarkable year, a voyage of discovery.

I am heartened by the fact that during my brief tenure to date, there have already been several significant victories for the privacy rights of Canadians:

- The federal government's anti-terrorism legislation has been amended to ensure that it encroaches on privacy rights only to the absolute minimum necessary to meet legitimate security objectives. As originally drafted, the legislation contained provisions that went far beyond their stated objectives. They would have given the Attorney General the discretion to deprive Canadians of all privacy protection, by issuing blanket certificates that could effectively have abrogated the *Privacy Act* and the *Personal Information Protection and Electronic Documents Act*. The Minister of Justice accepted my representations and introduced amendments that fully met my concerns.
- The opening of mail from abroad by customs officers of the Canada Customs and Revenue Agency, on behalf of Citizenship and Immigration Canada, has been restricted to make it much more respectful of privacy rights. The previous practice, based on an arbitrary and outdated weight-based distinction in the *Customs Act* between mail and parcels, was perfectly legal – but it was deeply wrong in terms of privacy. When letter mail was sent in the large courier-type envelopes required by premium delivery services, this alone made it heavy enough to lose the exemption intended to protect the mail of Canadians from being opened without a warrant. Following my discussions with the Minister of National Revenue, he caused the agency to revise its procedures so that the spirit of the law is respected. The outer

envelopes no longer count toward the weight used to distinguish between mail that is entitled to privacy protection, and parcels.

- Deeply flawed provincial "health privacy" legislation in Ontario, which in fact would have given the Ontario government carte blanche to violate health privacy rights, did not go forward. Because our privacy is indivisible – it cannot be respected federally and violated provincially – I accepted an invitation to testify about the proposed law before a committee of the Legislature. Unlike other witnesses who recommended amendments, I suggested that this bill was so fundamentally defective in approach that it would be best to withdraw it and start from scratch. The bill was allowed to die on the order paper. I am hopeful that its eventual successor will be more genuinely aimed at protecting privacy.

These developments give me confidence that the structure of Canadian privacy law, based on an Officer of Parliament/ombudsman with a mandate to oversee the privacy rights of Canadians, is a sound and effective one. With sufficient public support, which depends on presenting the facts cogently and persuasively, much good can be accomplished and much harm can be averted.

I came to this position determined to be an effective champion for the privacy rights of all Canadians. To achieve this, I deemed it necessary both to reinvigorate the Office of the Privacy Commissioner and to greatly increase awareness among Canadians about the privacy issues that affect their lives.

Accordingly, this Office has nearly doubled in size over the past year. When I joined in September 2000 we had 54 people on staff; as of November 30 of this year, our staff had grown to a total of 84 (97 including our corporate services). This was done for two reasons: to meet our new oversight responsibilities under the *Personal Information Protection and Electronic Documents (PIPED) Act* which came into effect in January 2001, and to create a new communications branch which is the key to raising the profile of the fundamental right of privacy.

Public awareness is indispensable to the effective carrying out of my role. As an ombudsman, I basically have two instruments at my disposal: persuasion and publicity. And, of course, persuasiveness is greatly enhanced if it is backed, whenever necessary, by the support of informed, alert public opinion.

Canadians need to know and understand their privacy rights, and to demand that they be fully respected. That is why, since taking office, I have placed great emphasis on my responsibilities as a communicator. I have to date delivered 35 speeches to diverse audiences across Canada, and given more than 210 media interviews.

PRIVACY IS THREATENED AS IT'S NEVER BEEN BEFORE.

Of course, I was aware before I was appointed that privacy is an important issue. I recognized it as a critical element of a free society, and agreed with former Supreme Court Justice LaForest that it was "at the heart of liberty in a modern state." And the argument that privacy is the right from which all freedoms flow – freedom of speech, freedom of association, freedom of conscience, to name just three – struck me as a powerful one.

But it didn't take me long in this position to see that privacy was even more important, and its protection more urgent, than I had realized.

This is a critical time to be Privacy Commissioner. Privacy is threatened as it's never been before. The alarm about "the end of privacy" has been sounded often enough in the past. But it's a sad fact that this alarm was easy for people to dismiss as exaggerated.

A reasonably informed person cannot dismiss it anymore. The technological means to eradicate privacy clearly now exist – not only computers and information processing technology, but also a panoply of technological wizardry from video cameras to facial recognition software to "smart" identification cards. And the motives exist – not necessarily nefarious motives. Indeed, the greatest threats to privacy often come not from those who want to do harm, but from those who argue quite convincingly that privacy must be sacrificed on the altar of some greater good.

Most of us can now easily envisage a world without privacy – not just envision it, but consider it possible and imminent, in a future that we will all live to see. We don't need a George Orwell to say, "Imagine what this would be like." It's beginning to happen all around us.

We're all confronted now with the real possibility of having to go through life with someone looking over our shoulder, either metaphorically or quite literally. We face the real and imminent prospect of having to live our lives weighing every action, every purchase, every statement, every human contact, wondering who might find out about it, judge it, misconstrue it, or somehow use it to our detriment.

That's not freedom. That, on the contrary, is a distinguishing characteristic of totalitarian societies.

Yet I remain concerned that many Canadians are watching but not seeing the assault on privacy. Their attention becomes focused only when their own privacy has already been violated – and by then it's too late. A person's privacy, once violated, can never fully be restored. If personal information about any one of us becomes known by someone who has no business knowing it, there is no way to retroactively make it unknown.

"If we react to terrorism by excessively and unnecessarily depriving ourselves of privacy and the freedoms that flow from it, then terrorism will have won a great and terrible victory.

The pressures on privacy rights have, of course, become even more acute in the wake of the September 11 terrorist attacks. In a climate of fear and uncertainty, it can become all too easy to believe that the more the state knows about everyone, the safer we will all be. That, in turn, can give an unwarranted new aura of legitimacy to what are precisely some of the greatest threats to privacy – for instance, proliferating video surveillance, widespread use of biometric recognition technology, or national ID cards.

These pressures are further intensified by the fact that a climate of fear not only invites invasions of privacy, it also tends to discourage or penalize dissent. In the face of the destruction wrought by the terrorists, anyone arguing against any measure that has even the vaguest appearance of enhancing security must accept the risk of being accused of irresponsibility.

And yet the world has always been a dangerous place, and the evolution of fundamental rights such as privacy should teach us that their greatest value lies in their ability to endure and protect us in times of the worst adversity. When there is no great incentive to violate a right, it is not so much a right as a fact of life. It is only when the temptation to pursue some goal by brushing everything else aside comes closest to being irresistible, that our society's commitment to protecting fundamental human rights is truly tested.

Privacy and the other cherished freedoms and values that define Canadian society are not frills or luxuries in the situation we face since September 11. They are what this situation is all about. If we react to terrorism by excessively and unnecessarily depriving ourselves of privacy and the freedoms that flow from it, then terrorism will have won a great and terrible victory.

By all accounts, the goal of the terrorist campaign now underway is to attack and undermine the whole nature of American society, and by extension of all democratic societies. That makes our freedoms and values, very much including privacy, the central target. Far from making us safer, every ill-considered reduction of those freedoms – every needless encroachment on privacy – would be a proof that terrorism works and thus an incentive for further mayhem.

My responsibility as Privacy Commissioner is to do everything in my power to help ensure that the fundamental human right, and fundamental Canadian value, of privacy does not in fact fall victim to terrorism.

In discharging this responsibility, I don't argue that privacy is an absolute right, or even that there is no need for privacy-invasive measures to meet the kinds of security threats that we're now facing.

But it is my duty to insist that the choices about any such measures must always be made calmly, carefully, and case by case, and they must be justified according to clear criteria. I have suggested that the following criteria are appropriate, for government and the private sector alike:

- Any proposed measure to limit or infringe privacy must be demonstrably necessary to address a specific problem.
- It must be likely to be effective in addressing that problem – in other words, it must be demonstrable that the measure will make us safer, not just make us feel safer.
- The degree of intrusion or limitation of privacy must be proportional to the security benefit to be derived. It mustn't be a sledgehammer used to kill a fly.
- Finally, it must be demonstrable that there is no less privacy intrusive measure that would achieve the same result.

Though it went through some initial growing pains, the federal government's legislative response to the threat of terrorism is at present, in my view, one that satisfactorily meets these tests with regard to privacy rights. I believe that the new *Anti-Terrorism Act* now strikes a reasonable and careful balance between security and privacy. I am continuing to put forward my concerns and recommendations with regard to subsequent legislation.

Still, there will undoubtedly be further challenges and threats to privacy in the months ahead, in the continuing aftermath of September 11. The choices we make will be of momentous importance.

In the days and weeks following the attacks, the general public got a good look at what privacy advocates have long been worrying about. They saw that there is a huge industry eager to manufacture and sell the technology of surveillance: video cameras, facial recognition systems, fingerprint readers, e-mail and Web monitoring, "smart" identification cards, location tracking. And they saw how many people are eager to argue that if you don't have anything to hide, you shouldn't mind revealing everything.

Over the past year, long before the tragic events of September 11, I have increasingly become convinced that privacy will be the defining issue of this new decade. That is a message I have repeated forcefully in my public appearances. Until recently, what I meant was that we are facing unprecedented and irrevocable choices with regard to privacy because of advances in technology and science, and those choices will determine the quality of our lives.

"I PREFER A MORE MODERN AND REFINED DEFINITION OF PRIVACY AS THE RIGHT TO CONTROL ACCESS TO ONE'S PERSON AND INFORMATION ABOUT ONESELF.

That remains true. But now more than ever, privacy will be the defining issue, because the choices we make about the balance between security and privacy will determine what kind of society we leave for our children and grandchildren. Even an Orwellian society devoid of privacy wouldn't be entirely secure – the most oppressive police state is still not immune to terrorism – but gradually depriving ourselves of our privacy rights in the name of safety would strip our lives of the dignity and freedom that are the hallmarks of our society.

We will inevitably see this in retrospect as the decade in which we had our chance to take a stand in asserting the crucial value of privacy and defending it against its assailants. I very much hope we will be able to recall it as the decade in which we seized that chance and took that stand.

Most people used to define privacy using some variant of the famous formulation of Samuel Warren and Louis D. Brandeis, as "the right to be let alone." That's still a useful definition, and it certainly captures the visceral sense that people have of the importance of privacy.

I prefer a more modern and refined definition of privacy as the right to control access to one's person and information about oneself. This definition better captures the nature of modern threats to privacy, which take place chiefly in the context of the collection and use of information about us.

That's why I've said so often in the past year that we're at a crossroads. The means by which we protected privacy in the past, or rather the means by which we could leave it to take care of itself, don't work well anymore, and they will work less and less well as time goes on.

Privacy used to be protected pretty much by default. When information about us was in paper records and scattered over many locations, compiling a detailed dossier on any individual was a daunting task. Unless you were famous, important or suspected of a grave offence, your privacy could be relatively safe without your having to make much effort to ensure it.

The move to electronic record-keeping has changed all that, eating away at the barriers of time, distance, and cost that once guarded our privacy. New surveillance technologies – cookies and Web bugs, video cameras, e-mail monitoring, smart cards, biometric identifiers, location tracking, drug testing – assail us wherever we turn. Strangers sitting at computer keyboards compile dossiers on us in seconds. Our activities and our interests, our purchases and our movements, our opinions and our habits are dutifully recorded, analyzed, and classified, for whatever use the highest bidder can dream up for them.

With the default protection vanishing, it's up to us.

> Privacy has to be seen, not as a selfish individual interest that has to give way before greater social needs, but as the shared, collective, social interest that it is.

As I mentioned earlier, one of the most interesting things I have observed in the past year is that the greatest threats to privacy seldom come from those who want to do harm.

They come from well-intentioned people who say that privacy needs to be sacrificed for some greater good – improved customer service, prevention of crime, the advancement of science, more efficient delivery of government programs, security.

Of course, sometimes privacy *does* have to yield to other social interests.

But we need to ask ourselves – and ask those well-intentioned people – what kind of society we would be serving, building, and promoting, if the destruction of privacy were too readily the price to be paid.

Privacy has to be seen, not as a selfish individual interest that has to give way before greater social needs, but as the shared, collective, social interest that it is.

That's why it's an important time to be Privacy Commissioner.

It's also an important time to have a new private sector privacy law. For almost 20 years, we've had legislation controlling the way the government collects and handles the personal information of Canadians. It's in the private sector that we are seeing the greatest explosion in collection of information and compilation of dossiers about us. It's there that it's most urgent that we assert control over our personal information.

Parliament passed the *Personal Information Protection and Electronic Documents Act* almost two years ago, and it began coming into effect on January 1st of this year. This *Act* is an important tool for Canadians to reassert control over their personal information, and to take a stand to protect and preserve privacy.

The *Act* applies to personal information collected, used, or disclosed in the course of commercial activities. At its heart is a model code for the protection of personal information, which was developed jointly by business, government, and consumer groups. The code is based on widely accepted principles of fair information practices, including those set out by the Organisation for Economic Cooperation and Development in 1980.

What the *Act* says, in a nutshell, is this:

- Apart from some very limited exceptions, no private sector organization can collect, use or disclose personal information about you without your consent.
- It can collect, use or disclose that information only for the purpose for which you gave consent.

- Even with consent, it can only collect information that a reasonable person would consider appropriate under the circumstances.
- People have the right to see the personal information that is held about them, and to correct any inaccuracies.
- There is oversight, through me and my office, to ensure that the law is respected. And there is redress if people's rights are violated.

The *Act* is coming into effect in stages. It has applied since January of this year to personal information, other than health information, of customers or employees of works, undertakings, or businesses under federal jurisdiction – principally banks, telecommunications, broadcasting, and inter-provincial or international transportation, as well as in the Northwest Territories, Yukon and Nunavut, where it applies to the whole private sector, which, under the constitution, is federally regulated.

It also applies to personal information – again, other than health information – when it's disclosed across provincial or national boundaries for consideration. "Disclosed for consideration" is legalese meaning that you get something in exchange for it – for example, through sale, lease, or barter. The personal information itself must be the subject of the exchange for the *Act* to apply.

The exclusion of personal health information was a last-minute compromise, and it's temporary.

When the law was working its way through Parliament, representatives from the health care sector expressed two distinct, opposite sets of concerns. Some wanted a tougher law, with stronger consent provisions and restrictions on subsequent uses of personal health information. Others argued that the law would constrain operational activities in health care, and wanted it to be more permissive.

But there weren't any fundamental problems or obstacles to overcome. Everyone recognized that personal health information had to be protected. Neither then, nor at any time since, has anyone produced specific, clear indications why the law as written cannot work satisfactorily. In fact, as then-Deputy Minister of Health David Dodge testified before a Senate committee:

> "I have been asking for about six months for some specific examples of things that would really go wrong if the bill comes into effect, as indicated, in a year's time. I have been pressing to determine what things would actually fall down, what we really could not do. Frankly, I have been surprised that despite the general criticism and uncertainty I have not been given examples of things that would go wrong. There is an unease and uncertainty because

> Personal health information – information about the state of our own bodies and minds – is arguably the most private information of all.

we are into new territory. However, I have not had examples of things that would actually go wrong."

It was eventually agreed that health information would be excluded from coverage under the *Act* for one year after its coming into force. This was to give the health sector additional time to adapt to the new law.

In recent months, there has been a determined lobbying effort by various powerful health sector interests to continue depriving Canadians of the health privacy protection they were promised would come into effect on January 1, 2002. Some have been pressing for an extension of the exemption or carve-out for personal health information. Others would like to see the law tinkered with in a variety of possible ways, including a separate regulatory regime that would bypass the provisions of the *Act* and truncate the oversight role of the Privacy Commissioner.

But two things have remained constant over the past year. First, there is still no substantive consensus, with some still arguing for a stronger law and others for a weakened one. And, second, no one has yet demonstrated specifically and persuasively what is wrong with the law as written.

Any delay or dilution of the health privacy protection that Canadians have been promised by Parliament would, in my view, be a great blow to privacy rights.

Personal health information – information about the state of our own bodies and minds – is arguably the most private information of all. Any inappropriate disclosure can have devastating consequences. Indeed, fear of losing control over their health information can deter people from seeking medical care at all, with detrimental results not only for them but also for society as a whole. That's why any privacy protection legislation that does not fully protect personal health information is scarcely worthy of the name. The one-year delay in this regard was more than long enough.

An even greater concern would be the effect that any delay or tampering with regard to health privacy protection could have on the effectiveness of the *PIPED Act* as a whole. People in the health field may argue that their sector has special and distinct privacy issues. But people in banking, transportation, telecommunications – indeed, any sector of the economy – could easily make the same argument.

That is why the law was drafted in terms of relatively broad principles and rules, with ample room for flexibility and interpretation in its application. If special exceptions were to be made for one sector such as health, every other sector could likewise start demanding individualized treatment and the whole edifice of the privacy law would be at risk of crumbling.

"It is important to note that the health care sector will still have another two years to prepare for the coming into effect of the *Act* in the areas that are presumably of greatest concern to it.

I am therefore very pleased that the Minister of Health, Hon. Allan Rock, confirmed to me in a letter dated September 24:

> "I do not support the creation of a separate regulatory agency to deal with personal health information under *PIPEDA.* The *Act*, as passed by Parliament just over one year ago, is clear that oversight, redress and audit responsibilities rest with the Privacy Commissioner. The Deputy Minister has also made it clear to stakeholders in the Health sector that we are not contemplating amendments to *PIPEDA* to create a separate Agency for the health sector, nor do we support a delay in the application of *PIPEDA* to the health sector."

I very much appreciate this recognition by the Minister of Health, on behalf of his department, of the vital importance of having health privacy protection come into effect as scheduled on January 1, 2002.

At the time of writing of this report, it does indeed appear that the *Act* will apply as written. On January 1, 2002, the personal health information held by federal works, undertakings and businesses about their customers or employees will be protected.

The sale or barter of personal health information across national or provincial borders will also be covered. Disclosures of personal health information across any borders for consideration (where the consideration is for the information) will be covered. And all businesses and organizations in Yukon, the Northwest Territories and Nunavut that collect, use, or disclose personal information in the course of commercial activities will have to protect personal health information as well.

It is important to note that the health care sector will still have another two years to prepare for the coming into effect of the *Act* in the areas that are presumably of greatest concern to it. That's because the *Act* will not apply to such directly health-related commercial services as doctors' offices, private clinics, laboratories and pharmacies until January 1, 2004, when it extends to all private-sector commercial activities within provinces, except where a province has passed substantially similar legislation.

There is, however, one issue that I consider appropriate to address at this time.

I know that members of the health community are understandably concerned about the possible impact of the *Act* on health research, since it involves personal health information and pecuniary considerations are not always absent. I want at this time to provide assurance that bona fide health research, carried out with appropriate sensitivity to the privacy rights of Canadians, has nothing to fear from the *Act* or my Office.

My position on this important issue will be as follows:

Personal health information is perhaps the most privacy-sensitive of all personal information, and as a general rule individuals must have the right to control who can collect, use or disclose this information, and for what purpose. At the same time, however, our society has a vital interest in the continuation and development of health research, which holds the promise of great benefits for all individuals.

The Purpose clause of the *Act* specifies that its rules are intended to balance "the right of privacy of individuals with respect to their personal information and the need of organizations to collect, use or disclose personal information for purposes that a reasonable person would consider appropriate in the circumstances."

In the case of health research, it appears clear to me that the appropriate balance is one that safeguards the genuine privacy interests of individuals while permitting the conduct of legitimate health research that uses information in ways that can have no possible impact on the individuals to whom it pertains. I do not believe that the *Act* was in any way intended to deter or impede such research, and my provincial and territorial counterparts with whom I discussed the issue this summer share this view.

Accordingly, I intend to interpret broadly the intent of paragraph 7(2)(c) of the *Act*, which permits an organization to use personal information without the knowledge or consent of the individual if "it is used for statistical, or scholarly study or research, purposes that cannot be achieved without using the information, the information is used in a manner that will ensure its confidentiality, it is impracticable to obtain consent and the organization informs the Commissioner of the use before the information is used." Paragraph 7(3)(f) makes a similar provision for the disclosure of personal information without knowledge or consent.

I will take the view that bona fide health research carried out by duly accredited organizations under appropriate safeguards does in fact constitute statistical or scholarly study or research, whether or not there is an element of pecuniary interest involved. Merely because research into a particular medical condition may receive funding assistance from an outside source that hopes to reap financial benefit from the discovery of an effective new medication, for example, does not, I believe, change its legitimacy as health research from the point of view of privacy rights.

With regard to the impracticability of obtaining consent for such research, I accept the view of the health research community that cost factors and/or the difficulty of obtaining consent from 100 per cent of a

"In short, soon we will have seamless privacy protection in Canada.

target population make it impracticable to obtain individual consent for many health research studies.

The *Act* requires that the information in question must be used in a manner that will ensure its confidentiality. I consider this requirement to be of paramount importance.

I will accordingly take the position that personal health information can be disclosed and used without consent for health research as described above, but only provided that it remains strictly within the confines of the research project and that it can in no way harm the individual to whom it pertains.

Without limiting the generality of the foregoing, I will consider it an absolute requirement that personal health information disclosed and used without consent for health research purposes can under no circumstances whatsoever find its way to the individual's employers, insurers, relatives or acquaintances, governmental or law enforcement authorities, marketers or any other third parties, nor can the individual be contacted as a result of this information by anyone other than his or her own physician or other primary health care provider, as the case may be.

I and my Office will maintain vigilant oversight over this requirement, and any breach of it would be considered, ipso facto, an extremely grave violation of the *Act*.

I am convinced that this approach will fully meet the intent of the *Act*, effectively protect the privacy rights of Canadians, and permit all legitimate health research to proceed without impediment.

The final stage for implementation of the *Act* will be in January 2004. At that time, it will extend to all commercial activities in Canada, with one important exception: where a province has passed substantially similar privacy legislation, the federal government may exempt organizations and activities in the province from the application of the federal legislation, and the provincial law will apply.

Federally regulated businesses in those provinces will continue to be governed by the federal *Act*. So will personal information in all interprovincial and international transactions by organizations in the course of commercial activities.

In short, soon we will have seamless privacy protection in Canada. All of the private sector will be required to comply with the federal law or a substantially similar provincial one.

One of the points about the new private sector legislation that I have made frequently this past year, especially to business audiences, is that it doesn't set Canada apart from the rest of the world. Similar legislation is found in most economically advanced countries worldwide, with the only significant exception being the U.S. Even there, the debate is less

I DECIDED AT THE OUTSET TO PUT A SPECIAL EMPHASIS ON COMMUNICATIONS.

about the principles than about the best means of observing them.

One of the reasons that this kind of legislation is being adopted is that when one country has it, it can only fully protect its citizens' information if the countries with which it trades have similar protections. To promote a better understanding of how we protect privacy in Canada, I have spoken and participated in conferences in Washington, at Harvard University, and in Brussels, Cambridge, and London, and I've engaged in dialogue with privacy and data protection commissioners from around the world.

When I was appointed as Privacy Commissioner, I looked at the situation we were facing: multiple threats to privacy in the name of reasonable social objectives, ever-diminishing expectations of privacy, a complex new law, and a public that, to some degree, seemed so accustomed to having its privacy whittled away that it was in danger of losing sight of privacy's meaning and importance.

Faced with all that, I decided at the outset to put a special emphasis on communications.

One of my first acts as Privacy Commissioner was to establish a new Communications and Strategic Analysis Branch in my Office, with responsibilities for researching privacy issues and reaching out to the public, to inform them and to get their views. And I personally have seized all available opportunities to spread the word, criss-crossing the country, to address conferences and meetings and give interviews to the media.

I have also ensured that the public can get accurate, current information from our Web site – for example, my speeches are available there as soon as I deliver them – and in published form. We've made available information packages on a variety of subjects including identity theft, the census, and, of course, how to access personal information and assert your rights under Canada's privacy laws. We've also published extensive guides for individuals and businesses on the new *Act* and how it will affect them.

I do this because it is profoundly important for Canadians to know their rights and to understand the implications of losing their privacy. And the simple truth is that I rely on public support in my role as an ombudsman, which is the primary way I protect Canadians' rights under the *Privacy Act* and the *Personal Information Protection and Electronic Documents Act.*

I do not have formal powers to force government institutions and private sector companies to respect people's privacy, or to make amends when they have failed to do so. I can go to the courts in certain instances, of course, but that's never an optimal solution. What I rely on is the power of public opinion. Few people, in government or in business, want to incur the public's wrath. The better informed the public is, the more its opinion will be respected.

"The past year saw an upsurge in surveillance activities, by governments and the private sector, that has pushed this issue front and centre.

I want to come back now, as I said I would, to some of the specific privacy issues that have preoccupied me this year.

Surveillance – actual visual surveillance – has long been a central concern of privacy advocates. The past year saw an upsurge in surveillance activities, by governments and the private sector, that has pushed this issue front and centre.

Privacy means being able to go about your lawful business without your every move being scrutinized and monitored. While we have to be very mindful of the more subtle privacy threats presented by modern information collection and management, it is imperative that we not lose sight of the gross violation of privacy that surveillance represents.

Video surveillance is everywhere, in public and private spaces. We've become conditioned to being watched and recorded when we enter a bank or a convenience store, move through an airport, or drive through an intersection. And now, alarmingly, we are seeing a growing inclination to monitor us as we walk on the streets of our cities and towns.

People occupying a public space must reasonably expect to be observed by others. But it's one thing to expose yourself to casual glances, or even interested notice, by your fellow citizens. It's another to find yourself under systematic, relentless observation, without cause, by agents of the state.

We haven't yet reached the same point as the United Kingdom, with its ever-increasing network of video surveillance – some two million video cameras, according to a recent report, watching streets, parking lots, housing developments, and shopping centres. Nor have we yet followed the lead of the U.S., where there are already instances of random video surveillance of public gatherings combined with biometric databases, to produce an electronic equivalent of the police line-up – with everyone required to participate, independent of any suspicion of wrongdoing.

But we have seen the installation of video surveillance systems aimed at public streets in Kelowna, B.C. (the subject of a complaint received by this Office), and similar systems are being planned for various other Canadian cities.

And biometric face recognition technology, in Ontario casinos and at Toronto's Pearson International Airport, also made the headlines this year. (In the latter case the headlines turned out to be wrong: my investigation revealed that the RCMP was using biometrics in a reasonable manner. My account of this is in Part One of this report.)

The rationale for surveillance is always the same: it increases security and helps deter crime. That's not something to be dismissed lightly. Whether it's bank robbery or the running of red lights, privacy advocates have no sympathy for people who hide behind privacy as an excuse for wilful violation of society's rules and laws.

But, as someone once said, the only place where a police officer's job is easy is in a police state. We cannot let legitimate concerns about security override a legitimate concern about privacy. If we sweep everyone into the net, if everyone is a suspect whose every movement can be monitored and perhaps recorded, analyzed, and filed away – just in case – we may well have done the utmost to prevent and control crime. But we will have done it at the unacceptable cost of a fundamental human right.

And if the state has no business monitoring the law-abiding nation, the private sector has even less. Yet, this year, a private security company in Yellowknife decided to make public surveillance its business, and aimed its video cameras onto a downtown street. That was enough to trigger a complaint under the *Personal Information Protection and Electronic Documents Act,* which applies to all private sector activities in the territories. My findings are described in Part Two of this report, but suffice it to say that I found that this was a contravention of the *Act*. I think we can all take some satisfaction from the fact that this company acted without the support of the city's officials, police force, or the public, and stopped conducting the surveillance voluntarily when the public reacted negatively.

What is far more disturbing is the situation in Kelowna, B.C. Here the RCMP, acting as a municipal police force, set up a video surveillance camera to continuously monitor and record everyone on a public street. Investigating a complaint that was made to me by the Information and Privacy Commissioner of British Columbia, I found this activity to be a collection of personal information that is in clear contravention of the *Privacy Act.*

But the RCMP is still continuing 24-hour surveillance through the camera, only without continuous recording. This puts it into technical compliance with the *Privacy Act*, which defines personal information as information about an identifiable individual that is "recorded in any form."

As I made clear in my finding, I consider this sort of video surveillance of public places to be an extremely serious violation of privacy rights even in the absence of recording. It is the very presence of video cameras, whether they are recording at any moment or not, that creates the privacy-destroying sense of being observed. As well, if a proliferation of video cameras is allowed to take place, it is virtually certain that function creep will lead inexorably to the linkage of these cameras

"WHAT IS CRUCIAL TO EMPHASIZE IS THAT THERE IS ABSOLUTELY NO EVIDENCE THAT VIDEO SURVEILLANCE ACTUALLY REDUCES CRIME, RATHER THAN MERELY DISPLACING IT TO OTHER LOCATIONS WHERE THERE ARE NO CAMERAS.

with biometric technology. This would eventually make it possible to identify anyone in a monitored public place at any time, or to monitor the whereabouts and activities of any given individual as he or she moves from place to place.

What is crucial to emphasize is that there is absolutely no evidence that video surveillance actually reduces crime, rather than merely displacing it to other locations where there are no cameras. In fact, a spokesman for the RCMP detachment in Kelowna, Corporal Reg Burgess, was reported in *The Vancouver Sun* of June 19, 2001, as stating that such cameras "do, in some circumstances, prevent crime, but they mostly displace crime."

This *Vancouver Sun* article goes on to report: "Burgess added that, by shifting crime away from Kelowna's downtown core into residential neighbourhoods, police will be alerted to criminal activity more quickly by homeowners."

Since my mandate is to oversee privacy laws rather than the laws of common sense, it is probably beyond my purview to comment on this stated RCMP policy of using video cameras to relocate crime from downtowns to residential areas.

However, I met recently with RCMP Commissioner Giulliano Zaccardelli and tried my utmost to persuade him to demonstrate respect for privacy rights by ordering the removal of the Kelowna surveillance camera.

In a letter dated November 27, 2001, Mr. Zaccardelli responded:

> "I am satisfied that in the case of Kelowna, the RCMP is acting within the scope of its duty to protect the community based on well articulated public safety concerns. The use of the cameras will prove to be a valuable asset to the community in suppressing criminal activity and making it a safer place to live."

I then asked Commissioner Zaccardelli for the data on which he bases his conclusion that this video surveillance is indeed effective in assisting the RCMP in its duty to protect the community, and particularly for the evidence that the camera in operation since last February is in fact "suppressing criminal activity" and is making Kelowna "a safer place to live." Specifically, I asked Commissioner Zaccardelli for statistics on the number of arrests arising from the use of the camera since last February, and for statistics comparing the overall crime rate in Kelowna during the months the camera has been in operation to the crime rate for the same period last year. He was not able to provide any such information.

I find this deeply disappointing. One would expect the Commissioner of the RCMP, in choosing to reject the strong recommendation of an Officer of Parliament on such an important matter, to base his decision on the

> I respectfully request the assistance of Members of Parliament and Senators in seeking to persuade Commissioner Zaccardelli to rethink his stance on this issue.

clearest factual evidence, not on unsubstantiated anecdotal conjecture, supposition or wishful thinking.

Even more important, one would expect Canada's highest-ranking police officer, the head of our national police force, to want his force to be exemplary in setting the highest standard of respect for privacy rights. It remains my hope that Commissioner Zaccardelli will come around to that view. If he instead retains his current position on this video surveillance, he will regrettably be setting the diametrically opposite example, to be followed by police forces across the country.

The level and quality of privacy in our country risk being struck a crippling, irreparable blow if we allow ourselves to become subjected to constant, unrelenting surveillance and observation through the lens of proliferating video cameras controlled by the police or other agents of the state.

For this reason, I respectfully request the assistance of Members of Parliament and Senators in seeking to persuade Commissioner Zaccardelli to rethink his stance on this issue. I consider this to be a matter of the greatest importance.

Video surveillance is the most obvious means by which we are being watched and monitored in public. But there are others. The location technology being inserted in cell phones can pinpoint a caller's location to within 50 metres. Geographical positioning technology can be used to locate vehicles. Electronic payments systems used on toll roads and bridges can be used to track the movement of vehicles.

So we have moved well beyond the kind of exposure that "going out in public" used to mean. When we are out in public, we are really out in public – nothing, it seems, can remain private any longer.

And, to add to the problem, as the definition of what is public and what is private becomes blurred, the assault on our public privacy extends to domains that we once considered unquestionably private. A growing number of sensory enhancing technologies – chemical sniffers, thermal imaging devices, night vision binoculars, sound wave receptors, portable x-ray devices – allow what goes on in closed, unquestionably private places to "leak" into public space. The infamous Kyllo case in the U.S., where a marijuana growing operation was detected by a thermal imaging device that captured heat transmissions from the house, shows just how blurred the distinction between public and private can be.

Again, privacy advocates are not advocates of crime. We recognize the good intentions of those who want to use surveillance to increase security. But our society can achieve its legitimate aims for security and prevention of crime without throwing away privacy and the fundamental civil liberties that flow from it.

"Employees don't sign away their fundamental human right of privacy when they enter into an employment contract.

These privacy invasive technologies must be confined to very limited and specific situations where the threat to public security is material, significant, and imminent, and they must be subject to prior judicial authorization – warrants, in other words.

Even the extraordinary growth in generalized surveillance of our public selves, by agents of the state, pales when we compare it to the explosion in surveillance of employees both in and away from the workplace. This is an issue that is of increasing concern to me.

As I told a conference in Toronto last April, workplace privacy is one of those issues that has come to the fore because the default protection of privacy no longer does the job. Privacy rights in the workplace are ill-defined because, until now, they have not had to be defined.

Managers have always wanted to ensure productivity and prevent liability. Even before Henry Ford and Frederick Taylor brought us the production line and "scientific management," managers were monitoring, measuring and conducting surveillance of their workforces.

But for a long time technology imposed a benign limitation on this. Workers were able to maintain a core of privacy in their work – just as they can maintain the privacy of their desk drawers, lockers, and personal effects – simply because monitoring and recording could so easily be overloaded with information.

That benign limitation began disappearing as computers became more common. The dream of perfect control and perfect security is, for all intents and purposes, achievable in the workplace, with technology that allows managers to monitor everything that moves and analyze everything that's recorded.

For some, the idea that employees have privacy rights in the workplace is unacceptable, since they are on the employer's time and property and using the employer's equipment. I don't agree. Employees don't sign away their fundamental human right of privacy when they enter into an employment contract. It may come as a surprise to some that a considerable number of judges and arbitrators agree with me on this.

Nonetheless, we've witnessed an extraordinary growth in surveillance in the workplace. This is particularly apparent in the U.S., where there are few privacy laws to protect employees. In January 2001, the American Management Association surveyed 1,627 large and mid-sized companies and found that more than 75 per cent of them videotape their employees or monitor their e-mail, Internet, phone calls, or computer files. This is up nearly 10 per cent from a similar survey last year.

> Electronic monitoring should never be allowed to substitute for – it can't substitute for – good management and supervisory practices.

There have been no comparable studies of the extent of employee surveillance in Canada; it's often simply assumed to reflect the situation in the U.S. That may be an incorrect assumption, partly based on a failure to understand the difference in Canadian laws.

And that failure to understand the difference in laws is frequent in Canada. For example, employers often cite potential liability for workplace harassment as a reason to conduct surveillance, especially of Internet and e-mail use. That reflects U.S. legal doctrine, rather than Canadian. In Canada, anti-discrimination legislation only imposes liability on an employer if it has failed to take reasonable steps to prevent harassment. That doesn't mean wholesale electronic monitoring of the workforce. It means having a good harassment policy, training employees, having good anti-harassment procedures in place (such as a harassment co-ordinator and a confidential complaints process), and acting quickly and effectively if harassment does occur – or if there is good reason to suspect it.

The other excuse I hear for wholesale electronic monitoring is the supposed "potential" of Internet connections for time-wasting and misuse of the employer's facilities. I don't accept that we should monitor employees because of a potential for time-wasting any more than we should monitor the law-abiding public because of the potential for one or some of them to commit a crime. Reasonable suspicion of wrongdoing should be the only justification for monitoring and surveillance of a workforce. Electronic monitoring should never be allowed to substitute for – it can't substitute for – good management and supervisory practices. If the only way an employer can know whether employees are working is to monitor them electronically, there's something wrong with his management practices.

The *Personal Information Protection and Electronic Documents Act* limits collection, use, and disclosure of information to "purposes that a reasonable person would consider appropriate." That's an important restriction on monitoring and surveillance in the workplace. Since the *Act*, or provincial legislation very much like it, will be binding on many employers throughout the country very soon, all employers should be looking at it.

I mentioned earlier the privacy implications of pressure for open government and access to government information. This came to a head this year in the attempt by various parties, supported by the Information Commissioner, to get access to the agendas of the Prime Minister.

That the values of openness and access to information could be twisted into such an attack on privacy – agendas are by their very nature private – has been a painful discovery for me. I never thought I would have to find myself opposing access to information. As a former journalist, I am acutely aware of the importance of openness in government. As an actively involved citizen, I have seen how accountability can be enhanced when information is readily available.

But this unquestionably good thing cannot bulldoze everything in its path, or justify a violation of individual privacy. Once again, privacy has to be asserted in all its societal importance, as a fundamental right, so that we don't see it as something that can be traded away every time someone sees it as an impediment to a valid objective.

Fortunately, I'm not alone in my concern about this. The courts have been very clear: open government doesn't preclude protecting fundamental human rights. Access is an administrative right that can enhance democracy. Privacy is a fundamental human right that is the very essence of democracy.

Another important issue is Government On-Line. The move to a seamless electronic interface between the citizenry and various levels of government can be an excellent development, improving the way programs are delivered and making government more efficient and accessible. Every Canadian has a story to tell about being confused as to which department or which level of government is responsible for which service. And many Canadians know the stories, whether true or apocryphal, of the difficulties that can be encountered in trying to get information from government.

But the walls between agencies and programs, within government and across levels of government, are also walls between collections of personal information. Government as a single, centralized body brings with it the prospect of merging databases of information about individuals' interactions with government. That information has been collected for specific uses. When it's held in separate databases specifically for those purposes, it's compartmentalized.

> Privacy has to be built into these Government On-Line projects from the start.

When those databases are merged, someone with a need to know only one piece of information can have access to lots more. And information can be combined, to reveal new information, leading to detailed profiles of individuals, tracking their activities and their interaction with government. Combine that with the assignment to each Canadian of an authentication, identification, and access device – what the government is calling "e-identities" – and we could find ourselves faced with a surveillance society, and the end of the right to be let alone.

Moreover, delivering services or benefits electronically will depend on private sector involvement. Private sector providers, as components of government delivery systems, could become repositories of vast databases on Canadians. That is cause for concern, given the limited protection of privacy in the private sector, even with the new private sector legislation.

I've addressed many audiences this year on this subject, and undertaken a continuing process of consultation with the Government of Canada. My message is simple enough: privacy has to be built into these Government On-Line projects from the start. That includes doing privacy impact assessments, and consulting with privacy protection agencies at the design stage – not late in the process, when the privacy problems are already locked in.

Again, I am not questioning the motives of the people behind these initiatives. I have no doubt that their intentions are the best. Efficiency is a worthwhile aspiration. But, as I have emphasized repeatedly, efficiency has to be properly understood, as a relation between means and ends – choosing the best means of achieving defined goals. What's critical is how we define the goals. For government, and for society, those goals have to include the preservation and protection of privacy.

Earlier, I touched on the issue of the privacy of health information. It is difficult to emphasize its importance enough.

Governments at both the provincial and the federal level intend to expand the collection and sharing of personal medical information and develop a comprehensive health information system. The intent is laudable – to deliver a consistent standard of care across the country, assessing why people get sick, and determining who is using, and abusing, the system and why.

But the result may be that a person's latest medical check-up has a potential audience of thousands. And because the state of the health care system is such an urgent concern, privacy issues could tend to be disregarded, or at least given short shrift, in the discussion.

Losing control over health information can have devastating consequences. Fear of losing control may discourage people from seeking medical care at all. The prospect of detailed psychiatric assessments finding their way into an insurance administrator's or an employer's hands, for instance, may be enough to dissuade patients from seeking care. Or they may withhold vital information from doctors, prejudicing the effectiveness of treatment and ultimately wasting the resources of the health care system.

Nearly 87 per cent of doctors in a recent survey in the U.S. reported that a patient had asked them to keep information out of their records. Nearly 78 per cent said they had withheld information from their records because of privacy concerns. We have to wonder whether attitudes are similar here in Canada.

For the patient, health information is fundamentally personal and sensitive. It needs the highest level of protection to ensure that it can never be used to the detriment of the individual to whom it belongs.

I remain very concerned about the security of sensitive medical information. Storing medical records electronically may increase the risks of not just a trickle of isolated privacy violations, but a full-scale flood. We've all heard about unintended disclosures of personal health information and security breaches on the Internet.

Take the recent example of the Eli Lilly and Company's unauthorized disclosure of 700 e-mail addresses of people taking Prozac. Eli Lilly had offered patients taking this drug an e-mail reminder service. The privacy breach took place when an e-mail, sent out at the end of June announcing the end of the program, listed all of the e-mail addresses of the people who had signed up for the service. This simple act created a lot of negative publicity for the company and contributed to the debate in the United States about the difficulty of protecting patient records that are stored electronically.

We also now have examples of hackers gaining access to hospital records. Back in December 2000, *The Washington Post* reported that a Dutch hacker had penetrated the patient record system at the University of Washington Medical Center in Seattle. The hacker is said to have downloaded copies of several thousand patient files containing patient names, conditions, home addresses and Social Security numbers. Closer to home, *The Vancouver Sun* reported in August that five pharmacists in

> Privacy is not an option, or a frill. It is a fundamental right.

British Columbia were recently disciplined and fined by that province's College of Pharmacists for spying on the medication records of colleagues, relatives, friends or acquaintances.

So are we, as a society, prepared for the privacy and security breaches that may be coming? Perhaps, at the very least, we should give patients the right to choose whether to have their medical records stored electronically. We recognize that electronic patient files represent great opportunities for quality of care. But we should also recognize that they represent a challenge from the perspective of patient privacy and confidentiality. The opportunities cannot be realized if the challenge is not met.

Indeed, this fact – that the opportunities of the future cannot satisfactorily be realized if the challenge of safeguarding privacy is not met – applies to all the issues with which I deal and which I have been addressing in this overview.

Privacy is not an option, or a frill. It is a fundamental right. The need to respect that right goes to the very heart of all our hopes for progress as a society and as individuals. That's because all meaningful progress is ultimately about improving the quality of our lives – and we must never delude ourselves that we can achieve such improvement if we pursue it, in any field, at the expense of heedlessly sacrificing the right to privacy which is so essential to our freedom and dignity.

Combating that delusion wherever it arises, and averting that sacrifice whenever someone tries to impose it on us, is what the work of my Office is all about. In the following sections of this report, I will provide an accounting of how we have been discharging our responsibilities.

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 rights to access and request corrections to their personal information. It also sets out my duties, responsibilities and mandate.

As Privacy Commissioner, I receive and investigate complaints from individuals who believe their rights under the *Act* have been violated. I also can initiate a complaint and 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 and 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 with the *Privacy Act,* I can, however, recommend changes to the way government institutions handle personal information, based on my investigation findings.

As well, as Privacy Commissioner, I have a mandate to conduct periodic audits of federal institutions to determine their compliance with the *Privacy Act,* and again, 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, 2000, to March 31, 2001.

Investigations

My Investigations and Inquiries 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'll talk about later in the report).

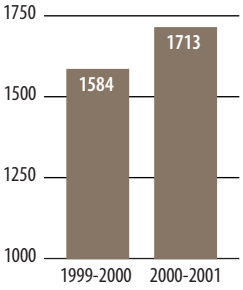
Through these investigations, I determine whether individuals' privacy rights have been violated or whether they've been properly accorded access to their personal information. Where people's privacy rights have been violated, I look for ways to provide redress for them, and prevent violations from happening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

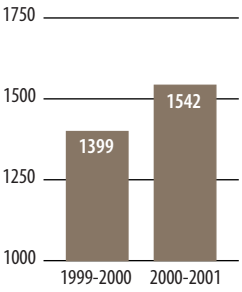
To date, all complaints under the *Privacy Act* have been resolved without our having to use these formal investigative powers, because voluntary co-operation with investigations has been forthcoming.

The 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.

Complaints Received
April 1, 2000 to March 31, 2001



Complaints Investigations Closed
April 1, 2000 to March 31, 2001



Complaints under the *Privacy Act*

Between April 1, 2000, and March 31, 2001, we received a total of 1,713 complaints under the *Privacy Act.* That's an increase of almost 10 per cent over the previous year. The type of complaints we received conformed to the established pattern: 60 per cent of them concerned either denial of access to personal information or issues of collection, use, disclosure, and disposal of personal information, and the remaining 40 per cent concerned failure to respect time limits, where federal organizations had not responded to a request for disclosure of personal information within the 30-day timeframe set out in the *Act*.

My staff closed 1,542 investigations, an increase of 10 per cent over the previous year. Of the cases closed, 339 dealt with issues of collection, use, disclosure, or disposal, while 630 dealt with access matters and 573 with time limits. These complaints were concluded as follows:

Not well-founded:	421
Well-founded:	553
Well-founded/Resolved:	82
Resolved:	44
Settled during the course of the investigation:	321
Discontinued:	121

Complaints about departments taking longer than they should to respond to access requests are always troubling – justice delayed is justice denied, and the time limits are in the *Act* for a good reason.

Several federal government institutions stand out for particularly often failing to meet the prescribed time frames when responding to individuals' requests for access to their personal information. These are the Correctional Service of Canada, the Department of National Defence, the Canada Customs and Revenue Agency, and Human Resources Development Canada.

I consider it of great importance that all government departments and agencies faithfully meet the time limit requirements set out in the *Privacy Act.* Respecting the lawful rights of Canadians is mandatory, not optional. There simply is no excuse for an entity of the Government of Canada to be breaking a law of Canada, and I intend to keep emphasizing this point.

Correctional Service of Canada

In the fall of 2000, in view of the number of time-limit complaints filed against the Correctional Service of Canada, I instructed my staff to address the matter with senior CSC officials. In February 2001, the Commissioner of Corrections agreed to implement measures to eliminate the backlog of requests in her department.

Those measures resulted in an improvement in the Correctional Service's handling of access complaints. In March 2001, the department had 1,684 active access requests in process, of which only about 20 per cent had been responded to within the prescribed time frame. By August 31, 2001, after an infusion of additional staff and overtime, the department managed to reduce the number of open requests to 501. Nearly 60 per cent of those were responded to within the prescribed time, and 30 per cent were overdue by 30 days or less.

There is no question that this is an improvement, and in July I ongratulated the Commissioner of Corrections for her department's achievement. The Correctional Service is continuing to work to reduce the number of outstanding requests and improve its response time. But while I am encouraged by these developments, they are not cause for euphoria. Nothing less would be acceptable.

Department of National Defence

Staff of my office began addressing the issue of timeliness with officials of the Department of National Defence in late 1999. At that time the department had approximately 2,100 outstanding access requests. The great majority of these were not processed within the prescribed time limit. Under pressure from my officials, the department agreed to implement measures such as hiring additional staff, making overtime available, and restructuring its internal procedures and organization.

These efforts have made some difference. As of November 2001, the department had reduced the number of outstanding access requests to 279. Of these, 136, not quite half, were not processed within the prescribed time limits.

Those numbers reflect an improvement, but the situation is still unacceptable. I recognize that, for the most part, the requests concern large files of information pertaining to things like police investigations, Boards of Inquiry, or harassment complaints. Such complaints are difficult to process. But that is a challenge, not an excuse.

Canada Customs and Revenue Agency

This agency has had significant problems responding to access requests in a timely fashion. Staff of my office met with representatives of the agency in early 2000, just as they had done with the Department of National Defence. The agency, just as National Defence had done, agreed to take measures, such as reorganization and hiring new staff, to improve the situation.

In the two fiscal years preceding this one, my office received 81 complaints of failure to respect time limits in one year and 127 in the next. Almost all (95 per cent in one year, 99 per cent in the next) were determined to be well-founded.

This fiscal year, the office received only 61 time limit complaints, and of those, 51 were well-founded.

Although they are better than the previous two years, these figures remain high. Again, the delays probably reflect the complexity of complaints about personal information in tax files, but further improvement is needed.

Human Resources Development Canada

We received 80 complaints against Human Resources Development Canada about failure to respect time limits. Of those, 47 – nearly 60 per cent – concerned access to personal information in the Longitudinal Labour Force File, the "super file" on Canadians that was dismantled last year because of privacy concerns. That was an exceptional situation, given the amount of attention the file received in the media and in Parliament, and the great volume of access requests the department had to deal with. If those exceptional circumstances are subtracted, we are left with 33 complaints about delays in responding to access requests. That number is still too high. But given the number of requests that the department receives in any year, and given the size of this department, the number is small enough to suggest that a bit of reorganization and extra work should suffice to eliminate it. The department needs to do so.

My Office will continue to monitor time-related issues and keep the pressure on for continual improvement.

Definitions 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 would 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 any formal finding in discontinued complaints.

Summary of Select Cases under the *Privacy Act*

Personal information found in DND dumpster

This case involved files full of personal information found in a trash bin outside an armoury. The files contained the personal information of dozens of Department of National Defence (DND) employees, including their names, home addresses and telephone numbers, dates of birth, medical and dental information, security-screening forms, employment histories, next-of-kin notification forms, performance assessments, and much more.

This information, if disclosed, could have resulted in real harm, and certainly substantial personal and professional embarrassment.

The person who found the files, an army reservist, reported his discovery to senior officers, but no action was taken. He was able to retrieve what he described as a small percentage of the files before the garbage bin was emptied, as usual, at the local dump. He gave the files to my Office and filed a complaint alleging that his personal information had been disposed of in an improper fashion.

My investigation established that an office was being moved to another floor and, in preparation, an order had been given to dispose of anything not needed in the new location. The office held parallel or "shadow files" outside the room where official DND files were kept. Some of the information in these shadow files was a duplicate of official files, some was not. The files were in plain folders without the departmental logo. As they didn't look important from the outside, no one thought to look inside them, and they were simply thrown out as trash.

Mixed in with these plain folders were a number of official DND files that included Candidate Progress Reports with detailed personal information.

Officials at DND reacted quickly, assuring my Office it would implement measures to eliminate the possibility of another occurrence of this nature. The department also agreed to reintegrate information found in the retrieved files into official departmental files.

While the use of "shadow files" does not contravene the *Privacy Act,* I'm very concerned about it. My Office repeatedly finds personal information held in such files throughout federal government departments. Often, the information is not disclosed to individuals seeking access under the *Privacy Act* because it is not maintained in the "official record."

An issue that came up during the course of the investigation was the Treasury Board of Canada guideline on the disposal of personal information.

This guideline describes three levels of personal information. The top level is personal information that, if compromised, "would cause extremely grave injury." Below that is a level that would cause "serious injury" if the information were compromised. The guideline recommends shredding as the method of destroying personal information at these levels.

Below that is what it calls personal information of "low" sensitivity. It defines this as personal information as that which, if compromised, would "cause injury."

According to the guideline, personal information of this type can be torn in half and disposed of in regular garbage containers.

I object strenuously to this guideline and its casual provisions for disposal of information that, by its own admission, could cause injury. I don't accept the distinction it makes between "injury" and "serious injury." Where privacy is concerned, any injury is serious. When personal information of any kind is to be destroyed, it should be shredded.

DND is not the only federal institution following this guideline. My discussions with DND security officials on this matter are continuing.

Personal information destroyed prematurely by HRDC

My investigation into this complaint found Human Resources Development Canada (HRDC) in violation of both the *Privacy Act* and its own Policy Manual.

An Employment Insurance claimant complained to me that his ability to obtain all the information he needed to file an appeal had been hampered by HRDC's destruction of the audiotape of the original hearing into his case by the Board of Referees.

HRDC's Policy Manual stated that such tapes were to be "kept for one year or until such time as the case has been heard by (the Office of) the Umpire, the Federal Court or the Supreme Court, as well, for any re-hearings of the Board of Referees, Umpires, etc." The complainant had been granted two Board of Referees hearings and had appeared before three Umpires (Federal Court judges), but had not exhausted all levels of appeal and was prepared to take the matter to Federal Court and the Supreme Court. Thus, in accordance with HRDC's own policy, the tape should not have been destroyed.

In addition, the *Privacy Act* and Privacy Regulations require government institutions to keep personal information used for an administrative purpose for a period of at least two years, to allow an individual an opportunity to access it.

As a result of my investigation, HRDC agreed to amend its Policy Manual to stipulate a two-year retention for audiotapes of its Board of Referees hearings. It also amended the manual to ensure that staff were aware of the requirements to keep the personal information for two years beyond hearings at every level up to and including the Supreme Court. An instruction was sent out to staff and the Appeals Division issued an amendment to the Policy Manual.

Concerns regarding release of information about groups by Statistics Canada

This complaint raised the interesting issue of "group privacy," which illustrates the need for caution when releasing information about identifiable groups. While disclosures of this kind may not identify any specific individual, they can still have an impact on personal privacy, because information about the group can diminish the privacy of every individual member of the group.

In this instance, a man who had received a series of telephone solicitations from brokerage firms filed a complaint against Statistics Canada, alleging that it had disclosed a sufficient amount of his personal information, obtained from the Canada Customs and Revenue Agency, to enable a research firm to determine his annual income.

The investigation revealed that the information sold by Statistics Canada to the research firm was in fact obtained from the 1991 Census, rather than from income tax records, as the complainant had alleged. And although the information did apply to a specific geographic area, it was not organized by postal code, as the complainant believed it to be. Nor was any of the information about identifiable individuals or personal information as defined in the *Privacy Act.*

In short, Statistics Canada did not contravene the *Privacy Act.* But the complaint did raise an important question about the privacy of members of identifiable groups.

Census products and services, even those based on information gathered from a 20 per cent random sample of the population, can provide a fairly accurate and detailed portrait of the characteristics of the population in a given geographic area. Research companies can and do combine information obtained from Statistics Canada with information obtained from other sources, such as telephone directories and consumer surveys, to compile profiles of specific areas.

When they can identify a relatively homogenous group in a specific geographic area, marketing companies can target individuals in that group, soliciting for everything from financial services to letters from charities.

The potential for damage goes well beyond simple annoyance. Consider the possible effect of a statistical study of a small neighborhood that has a high rate of mental health problems, for example, or a study of an identifiable group that has a high rate of HIV infection.

I have raised this with Statistics Canada. It says that while it makes every effort to ensure that individuals can't be identified in any of its statistical releases, it has established a working group to determine what measures it could take to address issues related to group privacy. It has indicated its willingness to explore this further with my staff. I look forward to further discussions with Statistics Canada on this matter.

New electronic system at National Defence compromised privacy of thousands

Failure to consider the privacy implications of a new electronic information system led to a situation in which any employee of the Department of National Defence (DND) could access personal information on thousands of military personnel. The situation could have been avoided if a few simple safeguards had been put in place.

This case provides a classic example of how easily privacy can be compromised by a well-intentioned attempt at more efficient management.

DND wanted to give managers a tool that would allow them to manage their staff more effectively. However, the project officers neglected to consult the department's privacy co-ordinator to ensure the system respected the requirements of the *Privacy Act.*

As a result, virtually any DND employee could visit the human resources section of the department's internal computer network and read or download detailed personal information about members of the Canadian Forces. This included date and place of birth, home address, marital status, the names and dates of birth of dependents, and results of linguistic testing.

Following the intervention by my Office, DND agreed to take corrective action to end this unjustified disclosure. It transferred the information to a site accessible by password only, with passwords distributed on a strict "need-to-know" basis.

DND also posted an electronic message on the human resources site asking users to destroy any information taken from the old site. I was concerned that this message might not reach all those who may have extracted or downloaded personal information from the file. I asked DND to take an additional corrective measure to trace users. The Assistant Deputy Minister, Finance and Corporate Services, sent a memorandum to all senior managers in National Defence asking them to warn all

employees to destroy any personal information originating from the original human resources site.

It's clear that in this case DND contravened the provisions on the use and disclosure of personal information set out in sections 7 and 8 of the *Privacy Act,* and violated the employees' fundamental right to have their personal information protected. Therefore, I concluded that this complaint was well-founded. Given that DND took satisfactory corrective measures to respect the requirements of the *Privacy Act,* I considered the complaint to be resolved.

Health Canada does not know if it disclosed personal information

An individual complained that a Health Canada doctor inappropriately disclosed his psychiatric assessment to his federal government employer, the Canada Customs and Revenue Agency (CCRA). CCRA had referred the man for a fitness-to-work assessment, which Health Canada does on behalf of federal government departments and agencies. To support his allegation, the complainant referred to a fax cover page indicating that Health Canada had sent an 11-page document to a human resources advisor at CCRA in October 1998.

A check of Health Canada's file confirmed that its doctor had indeed faxed 11 pages to CCRA at that time. However, the complainant's psychiatric evaluation was not found in CCRA's files. It was impossible to determine exactly what Health Canada did send to CCRA or even to confirm whether the fax had reached its intended destination.

If the investigation had confirmed that the evaluation had been sent to the employer, I would then have been required to examine the circumstances of the disclosure. My review would have focused on whether the disclosure met the requirements of the *Privacy Act.*

In this particular case, it is my view that there is a serious records management problem when a federal government department responsible for protecting sensitive medical information cannot determine what documents it sent by fax or whether they were sent to the appropriate individual.

To avoid a recurrence of this problem, Health Canada sent a note to directors of all regional offices reminding them that medical reports should not normally be delivered by fax. In those cases where fax transmission is necessary, it outlined a protocol to be followed in order to keep personal information secure. This protocol includes:

- Identifying the name and telephone number of the recipient;
- Listing contents of the fax on the cover page;

- Contacting the recipient by telephone prior to transmitting the fax to ensure the person is there to receive the document personally; and
- Asking the recipient to confirm receipt of the information in writing.

These principles should be followed by any institution that sends personal information over a non-secure fax line.

Information on vessel licences used to assess sales tax

A man on the West Coast bought a small boat and acquired a small vessel licence issued by Canada Customs officers. He complained that the Canada Customs and Revenue Agency shared the information on his licence application with the British Columbia Ministry of Finance, which proceeded to collect provincial sales tax on the purchase price of the boat. The complainant said he doubted many new boat owners realized their personal information would be disclosed in this way.

While small vessel licences are issued by customs officers, they do so on behalf of the Department of Fisheries and Oceans, which administers Small Vessels Regulations under the *Canada Shipping Act.*

The Department of Fisheries and Oceans' authority to disclose personal information without consent in this way is provided under an agreement between the Governments of Canada and British Columbia, which allows for access, use, and disclosure of personal information to administer or enforce any law. This is consistent with the provisions of the *Privacy Act,* and I concluded that this was a permitted disclosure of personal information without consent.

I did, however, have concerns about the transparency of the collection of the information. The Department of Fisheries and Oceans readily agreed to amend its licence application to advise boat purchasers that their information would be sent to provinces for assessment of sales taxes. The department has also agreed to review the agreement with a view to making it more specific.

No standard for disclosure of personal information to doctors

An individual complained that his employer, the Canada Customs and Revenue Agency, disclosed an excessive amount of his personal information to a psychiatrist.

The individual had presented a claim to the Québec *Commission de la santé et sécurité au travail* for stress-related leave allegedly resulting from the negative work environment created by the employer. The employer contested the employee's claim and requested the opinion of a psychiatrist through Health Canada.

The employer sent a letter to the psychiatrist explaining its concerns about the employee and attached a performance evaluation, which the employee had refused to sign, to support its contentions. The complainant alleged the negative appraisal should not have been disclosed and characterized the disclosure as an attempt by the employer to influence the psychiatrist's opinion.

Health Canada's Protocol for Special Fitness to Work Evaluation states that the employer must give the doctor a description of the problems and the reasons it has requested an evaluation, but says nothing on the issue of sending documents.

The Treasury Board of Canada's Policy on Occupational Safety and Health does not address what type of documentation should be provided to doctors. Nor does Info Source, a directory of federal personal information holdings and the key reference tool in place to assist members of the public in exercising their rights under the *Privacy Act.* Info Source does not address the use of appraisals for the purpose of sick leave or medical opinions. That means federal managers have no directives when it comes to sending documents to doctors performing evaluations on employees. This is not an acceptable situation.

Pursuant to discussions between my Office and representatives of Treasury Board and Health Canada, Treasury Board agreed to revise its Occupational Health Evaluation Standard to include the following directives:

- The employer is required to send the doctor only an explanatory letter.
- The employer must consult the doctor before sending supporting documentation.
- The employer must avoid using and disclosing personal information concerning third parties when submitting its reasons for requesting an evaluation.
- Where circumstances allow, the employer must meet with the employee to explain the reason for the medical opinion, inform the employee what information will be provided to the doctor and why, in order to ensure the transparency of the process.
- The employer must not use or disclose undocumented information such as hearsay or evaluative comments.

Treasury Board has also indicated that it will include this information in bulletins it prepares for the access to information and privacy co-ordinators in federal organizations subject to the *Privacy Act.*

Personal information of refugee claimant disclosed to another claimant

An immigration lawyer complained that the Immigration and Refugee Board disclosed personal information about one refugee claimant to another applicant. What makes this case interesting is that the lawyer was independently representing both clients. The Board gave him the woman's Personal Information Form, which she completed at the port of entry to support her refugee claim, in his role as counsel to the former spouse during his refugee hearing process. The Board notified the lawyer that the woman's form could be used during the spouse's hearing.

The two individuals had arrived at the port of entry together and indicated at that time that they were common-law spouses. The Board argued that the details each claimed were relevant in assessing not only his or her own credibility, but also the credibility of the other. It maintained that the use of this personal information in both claims was consistent with the original purpose of collecting the information, which was to assess their claims for refugee status. I agreed and considered the complaint to be not well-founded.

Nonetheless, this case raises important issues. The lawyer expressed concerns for women, particularly abused women, whose refugee claims are joined with those of other family members. This could mean a woman having to disclose sensitive, intimate details of abuse before a room full of relatives or former relatives. This could be a difficult, traumatic experience, one that would invade the privacy of an individual.

The Board's process does in fact provide for such circumstances. Claimants can make application to have joined claims treated separately. I was pleased to learn that in this case, the Board withdrew the woman's Personal Information Form when the lawyer objected.

The Personal Information Form will also be improved by adding a paragraph that clearly alerts refugee claimants to the possible use of their personal information in another hearing.

Selection boards and hand-written notes

The *Privacy Act* is clear: personal information used by a federal government institution to make an administrative decision about an individual is accessible to that individual, and must be kept for a minimum of two years.

This provision applies to the hand-written notes that members of selection boards take during employment interviews. Members of a selection board ponder their notes in reaching a decision on a particular individual's suitability for a position. That means that the notes have been used for an administrative purpose, and therefore must be retained for at least two years. This issue was addressed in several reports tabled by my predecessor.

In this instance, an unsuccessful applicant for a job with Fisheries and Oceans Canada, in order to prepare an appeal of the competition, requested access to the original, hand-written notes taken by selection board members. The department responded to the request by providing a copy of a typed summary report of its board members notes, and said it had destroyed the original notes upon completion of the competition.

After some deliberation, the department accepted my view that it had a responsibility to maintain its original notes on file. Department officials said there was no deliberate intent to deny access to personal information and assured me that policies have been amended to ensure that the original notes of selection board members are kept on staffing files.

Personal e-mail not necessarily private

A Department of National Defence (DND) employee questioned whether his employer was entitled to use and disclose his private e-mail messages in the investigation of a harassment complaint when those e-mail messages had been collected by improper means.

Someone had gained access to the complainant's computer and downloaded many of his e-mail messages. These messages contained personal information about the complainant, as well as derogatory comments about colleagues. The messages were printed and left on the desks of several employees. After reading the e-mails, these employees gave copies to their supervisor and lodged harassment complaints against the complainant.

The employer hired a consultant to investigate the harassment complaints and gave a copy of the e-mail messages to the consultant as evidence in his investigation. (A separate investigation failed to establish who had downloaded the messages.)

When the complainant learned that his e-mails had been provided to the consultant he complained to my Office, asserting that they had been improperly obtained in the first place, and that the employer had no right to use them in the investigation of the harassment complaints or to disclose them to the consultant.

This case raised important and timely issues. Although this was not a criminal investigation, it nonetheless raised a question about the use in an investigation of evidence that has been obtained unfairly, unethically, and possibly illegally.

That leads us to the whole question of workplace surveillance, and particularly the privacy of e-mail, a very hot topic in the last couple of years. As I mentioned earlier in this report, employers often claim that surveillance of e-mails is justified by the need to protect their employees against harassment.

I firmly believe that employers have to provide this protection. But I don't accept that protection necessarily translates into wholesale surveillance of e-mails or computer use. We accept that there are stringent limits on an employer's right to read employees' mail, eavesdrop on their telephone calls or rifle through their desk drawers. I think we have to look closely at e-mail communications to see what principles should apply there as well.

The Treasury Board of Canada's *Policy on the Use of Electronic Networks* incorporates the principle that the *Charter of Rights and Freedoms* protects employee privacy. It stipulates that institutions must put in place their own specific policy on the use of electronic networks. It further states that the policy should identify authorized and acceptable uses of the networks. The Treasury Board policy does not prevent monitoring if certain conditions apply.

DND's specific policy on the Management of Electronic Mail states that there should be no expectation of privacy on the part of employees when using e-mail systems. I find this deeply troubling. The law on privacy has developed around the notion of the "reasonable expectation"; one of the ways that the courts determine whether privacy has been violated has been to determine first whether a person could have reasonably expected privacy in a particular place and time. But I don't agree that it follows from this that an employee's, or anyone's, privacy can be simply eradicated by telling them not to expect any. While management has the right and the responsibility to manage, it has to operate within limits, including respect for fundamental rights. It is not for management alone to determine whether an expectation of privacy is reasonable.

In this specific case, I concluded that the employer had not contravened any provisions of the *Privacy Act,* and perhaps more importantly that it had not behaved unreasonably in the circumstances. I believe the complainant's expectation of privacy was lost once the e-mail messages had fallen into the hands of colleagues. The rights or wrongs of how that happened were not at issue, as I found no evidence that either the complainant's manager or his supervisor was responsible for monitoring or improperly gaining access to his e-mail.

The employer was authorized to hire a consultant to conduct the harassment investigation, and I concluded that it was authorized to provide the e-mails to the consultant. The e-mails were the basis of the complaints, so the employer could not reasonably have refused to provide them.

Lastly, I advised the complainant that employees who use the employer's electronic network in a manner that contravenes a departmental policy – in this case, to write derogatory messages about co-workers that

could be construed as harassment – should not expect their managers to ignore the inappropriate behaviour when it is brought to their attention. Again, how it was brought to their attention was not the issue. Had there been evidence that managers or supervisors had been responsible for gaining access to the complainant's e-mail, I might well have viewed the matter differently.

Incidents Under the *Privacy Act*

An incident is a matter that has been brought to my attention and warrants an inquiry but is not a formal complaint under the *Privacy Act.* During the period covered by this report, we looked into 21 incidents that came to my attention through various sources. The majority of these dealt with the inadvertent disclosures of personal information or perceived breaches of the *Privacy Act.* The following are some of the more striking examples.

Opening mail – right to privacy must be first consideration

In March 2001, it was revealed that Canada Customs officials were opening mail coming into Canada and passing the information on to Citizenship and Immigration Canada. The sanctity of personal correspondence is a cornerstone of privacy, and Canadians do not expect that their letters sent through the mail will be opened by anyone except the intended recipient. We don't live in one of those countries where mail is routinely opened by the authorities – or so we thought. I immediately looked into this matter.

Many people were surprised to learn that the opening of mail by Customs is lawful, if the mail weighs over 30 grams. If it is less than 30 grams, the *Customs Act* prohibits opening it without either a search warrant or the addressee's consent. But as long as the mail, whether a package or personal correspondence, weighs more than 30 grams, Customs inspectors may open it if they believe that it contains contraband or false documents. Any mail considered suspicious from an immigration standpoint is turned over to immigration officials for examination and further action.

It is of great concern to me that this arbitrary and artificial weight distinction allows the opening of, not just packages, but private correspondence. Correspondence should be treated with the greatest possible respect for privacy. The weight of the correspondence should not make a difference. Sending a letter by any form of "priority post" requires placing it in a large and comparatively heavy outer envelope that by itself can often put the item in the "over 30 grams" category. A letter should not be considered any less "mail," and less deserving of privacy protection, simply because the sender wanted to ensure its timely and safe arrival, or for that matter because it's lengthy and therefore heavier.

I made these concerns known to the Minister of Citizenship and Immigration, and made the following recommendations

- Where Customs officials detect, in an envelope weighing more than 30 grams, a solid object that appears to be something other than correspondence, opening it would fall within the normal activities of the Customs process.
- Where no solid object is detected and an envelope is detained only on suspicion that it may contain fraudulent documents, Customs should pass the mail to Immigration unopened. Immigration could then obtain a warrant to open it if it had reasonable grounds to do so.

The Minister of Citizenship and Immigration rejected the recommendations, citing the apparent difficulty of detecting some solid objects like laminated cards in envelopes, and the great volume of mail passing through a postal facility. Essentially, she argued that implementing the recommendations would demand greatly increased resources.

Since I could not reach a consensus with the Minister of Citizenship and Immigration, I turned my attention to the Minister responsible for the Canada Customs and Revenue Agency. My discussions with the Minister of National Revenue produced a resolution to this matter. Customs has modified its approach and now disregards the weight of courier-type envelopes in determining whether a mailing weighs more or less than 30 grams. Letters within such courier packages are treated as personal mail and not opened if the letters themselves are under 30 grams. I very much appreciate the National Revenue Minister's assistance in resolving this matter.

Health Canada and its list of would-be marijuana users

Health Canada contacted my Office after receiving a call from a newspaper reporter who said she had obtained the names of 128 individuals who had applied to the department for legal exemptions to obtain marijuana for medical purposes.

My investigation focused on two issues: determining the names on the list so that those people could be advised that their personal information had been compromised, and finding out how the list came into the reporter's possession.

The reporter refused to give the list to either my Office or Health Canada. As more than 160 people had applied for the marijuana exemption by the time this matter came to light, there was no way to determine the identities of the 128 people on the reporter's list. Health Canada had no choice but to notify all of the individuals that it had failed to safeguard their personal information.

In order to identify the source of the leak, Health Canada carried out an internal investigation. It found that internal security was not adequate. Virtually all employees in the Office of Controlled Substances had access to the names. Recommendations to improve security were implemented promptly. Now, access to the database is on a need-to-know basis and restricted through the use of passwords.

As for the list itself, following interventions by my Office, the reporter agreed to destroy it. The list has not been published and the reporter confirmed that no copies had been made.

I was satisfied with the security measures implemented by Health Canada and its efforts to sensitize employees to their obligations under the *Privacy Act*.

Completed firearms licence applications stolen from Justice Canada

As part of its efforts to promote firearms registration, Justice Canada's Canadian Firearms Centre runs Operation Outreach, a program to reach the owners of firearms in their own communities. Using storefront operations in malls and vans that travel to small towns and country fairs, staff help people fill out firearms licence applications and mail the completed forms to a licence-processing centre. In British Columbia, one of the vans was stolen. The van was recovered, but a box containing some 20 completed applications that had been in the van was missing.

Following news reports of the incident, I asked that the circumstances of the theft be examined along with the efforts undertaken by the centre to identify and notify applicants whose forms were taken. Not only had personal information gone missing, but that information could be used by unscrupulous individuals to obtain firearms licences they might not be entitled to have.

The centre appealed through the media for individuals to come forward if they had completed an application in the days before the theft. Only two did. The hope remains that other applicants will contact the centre once they realize they have not yet received their licence. As a long-term safeguard, the centre has updated its policy to ensure that completed applications are mailed to the Firearms Centre at the end of each day. Although this incident remains unresolved, I am satisfied with the centre's efforts at damage control.

Concerns about biometric identification technology

Biometric technology, which identifies people by their physical characteristics, is of special interest to my Office. When the media reported that the RCMP was using face recognition software to monitor travellers at Toronto's Pearson Airport and identify criminals, I launched an investigation immediately.

As it turned out, the report was wrong. The RCMP is not using surveillance cameras with biometric software, although the software is in use in the RCMP detention area at the airport to analyze photos of individuals who have been arrested. A photo of the individual under arrest is taken with a digital camera and stored on the hard drive of a stand-alone computer. The software takes point-to-point measurements of facial bone structure and compares this digital portrait of the individual under arrest against those already in the system. As bone structure cannot be altered as readily as hair or eye colour, the system may be able to spot individuals using various identities. This was a sophisticated version of the traditional mug shots used by law enforcement.

In this instance, I was satisfied that biometric software was not being used as the media reports suggested and no privacy concerns were identified.

Taxpayer received someone else's refund

A reporter for the *Calgary Herald* was handed a pretty good story when she received another person's income tax assessment and refund cheque in the same envelope as her own.

An investigation by my Office determined that a mechanical error at Public Works and Government Services Canada's Winnipeg Production Centre was to blame. The Winnipeg Production Centre prints and mails taxpayer assessments and cheques on behalf of the Canada Customs and Revenue Agency.

The plant is fully automated to print, cut, and fold assessments and cheques. The documents are put into envelopes, which are then sealed. The sealed envelopes pass under an optical detector that shines light through them and warns if an envelope is too thick.

This year however, due to changes in the grade of paper used and the number of pages of the form, the envelopes are thicker. The optical detector could not be adapted to accommodate these changes, and was inoperable.

Only one incident of this type has been reported. To help ensure the incident is not repeated, quality control at the plant has been tightened and there is increased random sampling of the final product.

I was satisfied by the steps Public Works took to prevent future errors of this type and by its offer of an apology to the individual involved.

Public Interest Disclosures

Under paragraph 8(2)(m) of the *Privacy Act,* the head of a government department may disclose personal information without the individual's consent where there is a compelling public interest that outweighs the invasion of the individual's privacy or where the disclosure

would benefit the individual. A "compelling public interest" often pertains to public safety and security, or to accountability to the public for decisions taken by departments.

Heads of departments are required under subsection 8(5) of the *Act* to provide me with written notice of any use of this provision. Ideally, this is done prior to the disclosure of the information. If appropriate, I may notify the individual concerned about the release of the information. In all cases, I attempt to ensure that only the minimum amount of personal information needed to achieve the public interest objective is disclosed.

During the period covered by this annual report, I received notice of 53 of these disclosures.

This past year, most notifications came from the RCMP, National Defence, Correctional Service of Canada, and the National Parole Board.

The RCMP made a number of public interest disclosures in relation to the release of sexual offenders into the community at the end of their custodial sentences. In most cases, the individuals' offences had involved children, and they were assessed as being at a high-risk to re-offend. Some had been deemed to be dangerous sexual offenders. Based on concern for citizens in the communities in which the offenders were released, the RCMP deemed the public disclosure of personal information to outweigh the harm caused by the invasion of the offenders' privacy.

On a number of occasions, National Defence disclosed information related to deaths on duty of Canadian Forces members. The information was released to the member's next of kin on compassionate grounds in the hope that a better understanding of the circumstances surrounding the death of their relative would help them achieve some level of closure.

Correctional Service of Canada and the National Parole Board publicly disclosed a number of Board of Inquiry reports dealing with issues such as escapes from federal institutions, breaches of statutory release requirements, and inmates' commission of further offences, including murder, while on release. These reports included personal information. Most of the cases had received significant media coverage. The individuals had been re-incarcerated, but because of the media coverage and the public scrutiny, Correctional Service of Canada and the National Parole Board considered it to be in the public interest to disclose the reports. The public disclosures were seen as necessary for the public to understand the events surrounding the incidents and the actions taken to prevent recurrence.

Top Ten Departments by Complaints Received

April 1, 2000 to March 31, 2001

Organization	Total	Access to Personal Information	Time	Privacy	Other
Correctional Service of Canada	672	136	342	194	
Canada Customs and Revenue Agency	197	91	59	47	
Human Resources Development Canada	190	63	88	39	
Royal Canadian Mounted Police	136	85	24	26	1
National Defence	100	40	46	14	
Citizenship and Immigration Canada	90	32	48	10	
Canadian Security Intelligence Service	40	37	2	1	
Canada Post Corporation	38	16	4	18	
Justice Canada	30	8	12	10	
Foreign Affairs and International Trade Canada	27	4	23	0	
Others	193	97	42	54	
Total	**1,713**	**609**	**690**	**413**	**1**

Completed Investigations and Results by Department

April 1, 2000 to March 31, 2001

Organization	Well-founded	Well-Founded/ Resolved	Not Well-founded	Discontinued	Resolved	Settled	Total
Agriculture and Agri-Food Canada	0	0	0	0	0	5	5
Auditor General of Canada	1	0	1	0	0	0	2
Canada Customs and Revenue Agency	64	15	57	6	28	60	230
Canada Mortgage and Housing Corporation	0	0	0	0	0	1	1
Canada Ports Corporation	0	0	0	2	0	0	2
Canada Post Corporation	5	1	5	0	2	11	24
Canadian Environmental Assessment Agency	0	0	0	0	0	1	1
Canadian Food Inspection Agency	0	0	0	1	0	2	3
Canadian Grain Commission	0	0	0	1	0	0	1
Canadian Heritage	0	0	1	0	0	3	4
Canadian Security Intelligence Service	0	2	43	0	0	2	47
Office of the Chief Electoral Officer	0	0	0	1	0	2	3
Citizenship and Immigration Canada	35	7	21	7	0	12	82
Office of the Commissioner of Official Languages	0	0	0	1	0	0	1
Correctional Service of Canada	262	23	59	48	2	63	457
Environment Canada	0	0	0	0	0	4	4
Finance Canada	1	0	0	0	0	0	1
Fisheries and Oceans Canada	0	0	1	0	0	1	2

Completed Investigations and Results by Department (Continued)

April 1, 2000 to March 31, 2001

Organization	Well-founded	Well-Founded/ Resolved	Not Well-founded	Discontinued	Resolved	Settled	Total
Foreign Affairs and International Trade Canada	3	0	4	1	1	3	12
Health Canada	5	0	26	1	1	2	35
Human Resources Development Canada	79	4	21	14	2	37	157
Immigration and Refugee Board of Canada	4	3	6	0	0	2	15
Indian and Northern Affairs Canada	4	0	2	0	0	5	11
Industry Canada	0	0	5	1	0	3	9
Justice Canada	2	0	43	3	0	8	56
Millennium Bureau of Canada	0	0	1	0	0	0	1
National Archives of Canada	1	0	7	6	2	12	28
National Defence	55	13	26	7	1	26	128
National Parole Board	1	0	3	0	0	7	11
National Research Council of Canada	0	0	2	0	0	0	2
Natural Resources Canada	0	0	0	0	1	0	1
Ombudsman National Defence and Canadian Forces	1	0	0	0	0	3	4
Pension Appeals Board	0	0	0	0	0	1	1
Privy Council Office	0	0	3	1	0	1	5
Public Service Commission of Canada	1	1	3	1	0	0	6
Public Service Staff Relations Board	0	1	5	0	0	0	6

Completed Investigations and Results by Department (Continued)

April 1, 2000 to March 31, 2001

Organization	Well-founded	Well-Founded/ Resolved	Not Well-founded	Discontinued	Resolved	Settled	Total
Public Works and Government Services Canada	8	0	6	1	0	2	17
Commission for Public Complaints against the RCMP	0	1	1	0	0	0	2
Royal Canadian Mounted Police	18	9	51	12	4	25	119
Social Sciences and Humanities Research Council of Canada	0	0	0	0	0	1	1
Solicitor General Canada	0	2	11	1	0	0	14
Statistics Canada	1	0	1	0	0	0	2
Transport Canada	2	0	0	1	0	3	6
Treasury Board of Canada	0	0	3	1	0	0	4
Vancouver Port Authority	0	0	0	2	0	0	2
Veterans Affairs Canada	0	0	3	1	0	13	17
Total	**553**	**82**	**421**	**121**	**44**	**321**	**1,542**

Completed Investigations by Grounds and Results

April 1, 2000 to March 31, 2001

	Well-founded	Well-Founded/ Resolved	Not Well-founded	Discontinued	Resolved	Settled	Total
Access to Personal Information	**11**	**73**	**241**	**54**	**36**	**215**	**630**
Access	11	70	229	51	15	207	583
Correction/Notation	0	3	12	3	21	5	44
Language	0	0	0	0	0	1	1
Inappropriate Fees	0	0	0	0	0	2	2
Privacy	**45**	**9**	**124**	**58**	**8**	**95**	**339**
Collection	3	0	28	33	2	32	98
Retention and Disposal	2	2	9	0	4	7	24
Use and Disclosure	40	7	87	25	2	56	217
Time Limits	**497**	**0**	**56**	**9**	**0**	**11**	**573**
Correction/Time	15	0	1	1	0	0	17
Time Limits	473	0	31	8	0	10	522
Extension Notice	9	0	24	0	0	1	34
Total	**553**	**82**	**421**	**121**	**44**	**321**	**1,542**

Origin of Completed Investigations

April 1, 2000 to March 31, 2001

Province/Territory	Number
Newfoundland	5
Prince Edward Island	3
Nova Scotia	103
New Brunswick	50
Quebec	306
National Capital Region – Quebec	11
National Capital Region – Ontario	177
Ontario	347
Manitoba	82
Saskatchewan	63
Alberta	109
British Columbia	267
Nunavut	0
Northwest Territories	3
Yukon	9
Outside Canada	7
Total	**1,542**

Inquiries by type under *Privacy Act*

April 1, 2000 to March 31, 2001

Subject	Number
Adoption, genealogy, missing persons	31
Census	45
Criminal records, pardons, U.S. waivers	190
E-311 Travel Declaration Form	39
Firearms	44
Longitudinal Labour Force File	68
Medical Records	91
From Members of Parliament	27
No jurisdiction, federal	427
Privacy Act, interpretation and process	6,460
Public Affairs (media, publications)	896
Redirect to provincial commissioners	1,068
Redirect to other federal agency	651
Redirect to other	499
Register of Electors	21
Social Insurance Numbers	746
Other	296
Total	**11,599**

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 like 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 the Canadians' privacy rights are respected.

In the next few pages I describe three key cases concerning the personal information-handling practices of federal institutions.

Personal documents not shredded – Golden West Document Shredding, Inc.

I have spoken many times about the need to develop a "culture of privacy" within organizations, both public and private. Whenever I read a magazine article about privacy, look at a conference agenda, or review the latest survey on people's privacy concerns, the focus is almost always on the private sector. That focus

is appropriate, but we should not lose sight of the enormous diversity of personal information that governments collect, use, and share. In fact, many of the most serious threats to privacy continue to come from governments.

Unlike businesses, governments have the power to demand personal information from their citizens. They collect information using the force of law. When a government agency or program needs personal information to carry out its mission, that information will be collected. Individuals have no choice in the matter.

As citizens, we must interact with government in order to participate in social programs, receive public assistance, and contribute to the public good through taxation regimes. In doing so, we entrust government with some of our most sensitive personal information. Whether applying for employment insurance, filing income taxes, registering firearms, or filling in census forms, individuals are not in a strong position to oppose the collection or use of their information.

So government must be particularly vigilant in maintaining the trust that citizens place in its ability to preserve the security and confidentiality of records that document individuals' lives and their identities as Canadian citizens.

The following finding represents a significant betrayal of that public trust, and provides a glaring demonstration of what can happen when cost and expediency are given precedence over privacy.

More than 30 federal departments and agencies had stored records at the Pacific Region Federal Records Centre of the National Archives of Canada. The centre was holding, literally, tonnes of highly sensitive personal information. The normal procedure is to destroy these records following a required retention period. A *Vancouver Sun* journalist informed us that a private sector company, hired to shred and recycle the records, was instead offering the material for sale to the highest bidder – *intact*, because whole paper brings a higher price than shredded paper on the recycling market.

Investigation revealed that between January and mid-July 1998, the National Archives had sent several hundred tonnes of material to Golden West Document Shredding, Inc. in Burnaby, B.C., for destruction. This was in addition to material Golden West had obtained directly from other federal government institutions. The following partial list catalogues some of the types of records involved and demonstrates the extent to which the privacy of Canadians may have been compromised:

- From Canada Customs and Revenue Agency, more than 22,000 boxes of material including tax returns, T4 slips, statements of investment income;

- From Human Resources Development Canada, claims for employment insurance benefits, employment counselling client files, applications for old age security and guaranteed income supplement;
- From Statistics Canada, census employment records, census interview records, surveys of employment and other surveys;
- From Public Works and Government Services Canada, employee pay records, cheque registers, payroll registers;
- From Citizenship and Immigration Canada, immigration case files.

If this information had fallen into the wrong hands, the consequences could have been disastrous for thousands of Canadian citizens. Detailed personal information, such as social insurance numbers, dates of birth, bank account numbers and home addresses, is a valuable commodity. In the proliferating crime known as identity theft, it is used by criminals to obtain credit cards, open bank accounts, redirect mail, rent vehicles, and even secure employment. Victims of identity theft often incur substantial financial losses, and must expend great efforts to restore their credit and reputation.

My staff found clear evidence that managers at both Public Works and the National Archives knew about the shredding company's serious financial, security, and technical problems before granting it security clearance to transport and shred classified federal paper waste. Moreover, the company that received the shredding contract was not even the same company that had made the original bid. The bid was submitted by "Golden West Document Shredding Inc.", a bankrupt company, and not "Golden West Document Shredding (1995) Inc.", which was awarded the contract. This inconsistency either went unnoticed or was ignored.

The Public Works security officer responsible for inspecting Golden West's facilities concluded that the company was barely meeting minimum requirements to obtain a facility security clearance. But he granted clearance after the manager of the National Archives Federal Records Centre assured him that National Archives would inspect the facility regularly and report any problems to Public Works.

Inspections, as it turned out, were insufficient to prevent the company from selling unshredded classified documents. In July 1998, during a surprise visit to the Golden West shredding facility, employees of Public Works and the National Archives found that approximately 95 tonnes of unshredded classified material had been sold to a paper-buying company, and was baled and prepared for shipment overseas and to the U.S. for recycling.

The RCMP investigated and reported to Public Works, but the report was not made public,

and my office was not informed of this alarming situation. Information we received from the RCMP during our investigation indicated that, before the material was seized at Golden West in July 1998, a recycling company had purchased four truckloads of government information. Two loads had been shipped via truck to the U.S. and another two loads had been shipped overseas, one to South Korea and another to the People's Republic of China. The RCMP was not able to determine whether the material was shredded.

In my findings after investigation, I agreed with the conclusions of the RCMP: responsibility for this incident rested squarely on the shoulders of National Archives and Public Works. Both had failed to exercise proper care in selecting Golden West. Both had failed to carry out their responsibilities to protect the highly sensitive personal information of thousands of Canadians.

The contract with Golden West came about because National Archives had decided to discontinue its in-house disposal service for classified paper waste for government departments. That decision was made in an effort to cut costs. But it was made without paying serious attention to protecting privacy. Monetary savings cannot override the legal obligation to protect individuals' personal information. The National Archives, acting on behalf of other departments and agencies, was fully responsible for the security and confidentiality of all the information until the paper was rendered unreadable. Both the National Archives and Public Works (as the contracting authority) were obligated to ensure the contractor was disposing of the records properly.

The National Archives has a vital role to play in ensuring that classified government records are properly destroyed at the end of their life cycle. It must provide leadership in the setting of standards and practices for records and information management for the Government of Canada. Requiring departments to make their own arrangements for classified waste disposal substantially increases the risks. This incident never would have occurred had the National Archives continued to shred waste at the regional records centre or had federal employees monitored the destruction at all times.

From a risk management perspective, the best solution would be to re-establish on-site shredding of sensitive records by the National Archives. An alternative could be the use of private off-site shredding services, but only if they can guarantee adequate security measures, and only if the shredding is under constant supervision of Archives staff. I understand the substantial resource implications of these options for the National Archives, and I would be prepared to discuss any other equally effective proposals.

Based on the findings of this investigation, I have made a series of recommendations to the National Archives and Public Works, and have requested that they provide my office with a report on how these recommendations will be implemented. I have also asked that in the future they notify my office, without delay, of any accidental or improper disclosure of personal information.

In addition, I have brought my concerns about the security and confidentiality of personal information that is to be destroyed to the attention of the Treasury Board, which is responsible for setting the Government of Canada's Security Policy and ensuring that it is followed by departments. As a result, the Board agreed to carefully examine the recommendations in my report that relate to either the security policy or the particular standard on contract security in the context of the current review of the Security Policy of the Government of Canada with a view to reducing the likelihood of such an incident reoccurring.

Privacy concerns at Canadian Firearms Program

My Office has taken a keen interest in the Canadian Firearms Program since the mid-1990s – naturally, since the program involves the collection and use of large amounts of highly sensitive personal information. The Office identified a number of potential privacy concerns when the concept was first proposed, suggested several changes to protect privacy when the legislation was before Parliament, and provided further comment when the subsequent regulations were attached to the legislation. Not one of our suggestions was accepted.

My Office continues to receive numerous inquiries and complaints about this program, including some from Members of Parliament. My predecessor initiated a review in January 2000 of the personal information-handling practices of the program. That review has now been completed. Based on it, my chief privacy concerns about the program relate to two areas: access and correction rights, and the collection and use of personal information.

The right of access and correction is especially critical because inaccurate or unsubstantiated information in the Firearms Interest Police database, for example, can lead to delays, licence refusals, or unnecessary questioning of neighbours and acquaintances. (The Firearms Interest Police database was created in 1998 to meet the objective of section 5 of the *Firearms Act* with respect to ineligibility to hold a licence. More than 900 law enforcement agencies across Canada feed incident-reporting codes into the National Police Services Network, which then serve as flags in the database during the application-screening process.)

For individuals exercising their right of access to and correction of their personal information held by the Firearms Program, it's proving

to be difficult and time consuming. The multi-jurisdictional nature of the program sometimes results in them having to go from one department or agency, or one level of government to another, to access their personal information.

An individual in a province such as Ontario, for example, where there is provincial and municipal privacy legislation, could be required to submit as many as three separate access requests in order to obtain the personal information related to one firearms licence application submitted at the federal level. The situation is worse for residents of Prince Edward Island, who do not yet have a legislated right of access to their personal information held at the provincial level.

With respect to the collection and use of personal information, my review revealed that the controls limiting access to the Police Information Retrieval System, for example, are inadequate. Firearms officers have access to more information than they need to make decisions about the eligibility of applicants. They also have access to personal information about other individuals, such as witnesses, acquaintances, and victims. These individuals are not applying for licences. The information about them would not normally be relevant to program requirements.

Another problem is that firearms officers rely on information collected from the Police Information Retrieval System database without verifying the accuracy of the information with the originating police agency. This is contrary both to established RCMP policies and to section 6(2) of the *Privacy Act,* which requires that personal information be accurate, up-to-date and complete. The review also revealed that some of the information being collected from police databases for the Firearms Interest Police system relates to incidents that do not qualify under section 5 of the *Firearms Act* or that are based on unsubstantiated information.

I also assessed the personal history questions on the firearms licence application form to determine if they are consistent with the *Privacy Act*'s restrictions on the collection of personal information.

In my view, the Firearms Program has not provided a demonstrable need for all of the questions. I have concerns about the highly intrusive nature of these three questions:

- "19(d) During the past five years, have you threatened or attempted suicide, or have you been diagnosed or treated by a medical practitioner for: depression; alcohol, drug or substance abuse; behavioural problems; or emotional problems?
- 19(e) During the past five years, do you know if you have been reported to the police or social services for violence, threatened or attempted violence, or other conflict in your home or elsewhere?

- 19(f) During the past two years, have you experienced a divorce, a separation, a breakdown of a significant relationship, job loss or bankruptcy?"

I have recommended that questions 19(d) and 19(f) should be eliminated and that question 19(e) should be revised to eliminate the references to "other conflict" and "elsewhere" and to eliminate the ambiguity.

While my review also raised some issues relating to the disclosure of personal information and security measures, I found that the physical, personnel, and information technology security measures are appropriate to the information being protected. But the review revealed that the Firearms Program had not yet implemented policies, procedures and practices with respect to the retention and disposal of program records.

Based on this review, on August 29, 2001, I made 34 recommendations for corrective measures relating to the program's overall personal information management practices. While I have received positive comments from the Royal Canadian Mounted Police, I have yet to receive any response from the Department of Justice.

The review did not address issues that have arisen subsequent to the research and fieldwork that formed the basis of this review, including outsourcing issues and any international information-sharing agreements. In addition, this review did not cover the handling of personal information by the Canada Customs and Revenue Agency. Since January 1, 2001, the Canada Customs and Revenue Agency has been responsible for administering part of the *Firearms Act,* involved in customs declarations and the movement of firearms. At the time of my review, this part of the *Act* was not yet in force. We're currently looking into these aspects of the program.

New databank protocol in place following Longitudinal Labour Force File

Human Resources Development Canada (HRDC) dismantled its Longitudinal Labour Force File in May 2000, after an outpouring of public anger about it. Since then, HRDC has implemented a strict protocol for all future research projects by any of its offices.

The protocol applies to all policy analysis, research, and evaluation activities that require the linkage of separate databanks. It also applies to linking with external data, including activities with an external contractor. It also covers the use of unmasked personal identifiers for survey purposes, whether the survey is conducted by HRDC, a contractor, or Statistics Canada, and whether the source of the data is an internal (i.e., HRDC) or external databank.

Beyond the fact that HRDC will not carry out linkages except for policy analysis and research that are consistent with its legislated mandate, the main feature of the protocol is to seek a balance. It is guided by principles relating to the public interest, including confidentiality, transparency, an assessment of the public good and avoidance of potential harm to individuals and identifiable groups.

I am pleased to see that HRDC recognizes that linking data from separate databases is intrinsically intrusive of privacy. HRDC will only consider such undertakings where the benefits are clearly in the national public interest. Another requirement is that the objective of the project should not be detrimental to the individuals involved or to identifiable groups, in that it cannot be used to make administrative decisions about them.

The protocol also stipulates that the dissemination of information relating to database linkage will be done in accordance with the confidentiality provisions of the *Human Resources Development Act,* the *Privacy Act,* the *Employment Insurance Act,* the *Income Tax Act,* the *Canada Pension Plan* and the *Old Age Security Act,* and with disclosure criteria contained in agreements with the provinces, territories, and other government departments and agencies.

I'm also pleased to see that, among other safeguards, all links among databases will have to satisfy a prescribed review and approval process. This involves the submission of documented proposals to an internal expert committee, the Databank Review Committee, composed mainly of senior HRDC officials. This review process includes consultation with my Office on all such projects, as well as with external partners when the project requires the linkage of HRDC databases with external data. Finally, the recommendation of the Databank Review Committee is forwarded to the Deputy Minister of Human Resources Development, who is responsible for the approval of each project.

HRDC is currently working on a legal protection framework that will govern the future collection and use of data and information obtained from Canadians, to be used by HRDC for its specific research requirements. It will include penalties for misuse and will be done in a manner consistent with federal laws, policies, and procedures, and with the outcomes of any government review of the *Privacy Act.*

Since September 2000, we have provided comments to HRDC on more than a dozen submissions, including the Canada Out-of-Employment Panel Survey, Canada Student Loans Programs-Key Performance Measure, and the Employment Benefits Support Measures Program.

Overall, I am satisfied that, under its protocol for databank linkages and its proposed legal protection framework, HRDC has addressed the concerns that my Office expressed about the Longitudinal Labour Force File.

Reviews

Immigration and Refugee Board and Canadian Nuclear Safety Commission

Reviews of personal information-handling practices under section 37 of the *Privacy Act* were initiated near the end of this fiscal year at the Immigration and Refugee Board and the Canadian Nuclear Safety Commission. These reviews include on-site visits in the National Capital Region and in selected regional offices across Canada. The reviews should be completed during the fiscal year of 2001-2002.

In the Courts

Introduction

My Legal Services Branch, headed by the General Counsel, provides me with specialized legal and strategic advice and litigation support with respect to the *Privacy Act* and the *Personal Information Protection and Electronic Documents Act.*

Section 41 of the *Privacy Act* allows an individual, following my investigation, to apply to the Federal Court for review of the decision of a government institution to refuse access to personal information. From the time the *Privacy Act* came into force in 1983 to March 31, 2001, 106 applications for review have been filed in the Federal Court. Six of these were filed in the past fiscal year.

Section 42 of the *Privacy Act* allows me, following completion of my investigation, to apply to the Federal Court for review of the decision of a government institution to refuse access to personal information, if I have the consent of the individual who requested the information. Three applications have been brought by previous Privacy Commissioners from 1984 to fiscal year end 2001.

Previous Commissioners and I have also intervened before the courts on a total of six occasions from 1984 to the present in applications brought by others, under either the *Access to Information Act* or the *Privacy Act.*

Recent Decisions

Privacy Commissioner v. Canada Labour Relations Board

This was an appeal by my predecessor from the decision of the Federal Court Trial Division. The case centred on notes taken by members of the Canada Labour Relations Board during the hearing of a complaint of a breach of a duty of fair representation. My predecessor argued that the notes, which contained personal information of the requestor, were under the control of the board and therefore subject to a right of access under the *Privacy Act.*

The appeal was heard on May 9, 2000, and the decision was delivered from the bench.

The Federal Court of Appeal held that the board members' notes were not "under the control" of the board for purposes of paragraph 12(1)(b) of the *Privacy Act.* The court stated: "These notes are being taken during the course of quasi-judicial proceedings, not by employees of the board, but by Governor in Council's appointees endowed with adjudicative functions which they must perform not as agent of the board, but independently of other members of the board including the chairperson of the board or a government institution. The principle of judicial independence and its corollary, the principle of adjudicative privilege, as applied to administrative tribunals, lie at the heart of the board's lack of control over the notes as a government institution."

My predecessor did not appeal this decision.

Information Commissioner of Canada (Appellant) v. Commissioner of the RCMP (Respondent) and Privacy Commissioner (Intervener)

This case involved the balance between the *Access to Information Act* and the *Privacy Act.* A list of postings of four named RCMP officers had been requested under the *Access to Information Act.* The Commissioner of the RCMP refused to release the information, on the ground that it related to the employment history of these individuals and was therefore personal information as described in paragraph (b) of the definition of personal information in section 3 the *Privacy Act.* The Information Commissioner applied in court for a review of the refusal.

At issue was whether the information could be disclosed pursuant to paragraph (j) of the definition of "personal information" in section 3 of the *Privacy Act,* which says that information relating to the position or functions of government officers or employees is not personal information.

The Federal Court of Appeal held that the information in dispute was personal information to each officer and was not within the paragraph (j) exception to the definition of "personal information."

The court rejected the RCMP's argument that the exception in paragraph (j) only applies to the current position of a government employee (or to the last position held in the case of a former government employee). The court agreed with the Information Commissioner and myself that paragraph (j) can apply to past positions.

The court rejected the argument of the Information Commissioner that one should take an expansive view of the exception found in paragraph (j) to justify the release of the requested information. The court adopted my position, stating that the exception should be construed in a way that does not allow for the disclosure of an individual's "employment history."

The Information Commissioner has obtained leave to appeal this decision to the Supreme Court of Canada. I will seek to intervene in the appeal.

Ongoing cases

Traveller Declaration Forms (form E-311)

The following two cases concern the disclosure of personal information by the Canada Customs and Revenue Agency (CCRA) to the Canada Employment Insurance Commission for use in an investigative data match program. The personal information in question was taken from Traveller Declaration Forms (E-311 forms) presented to Customs by Canadian residents between 1994 and 1996. The purpose of the data match was to detect employment insurance beneficiaries receiving benefits while out of Canada. The *Employment Insurance Act* requires claimants to be available for work, and disentitles them from receiving benefits if they are absent from Canada.

Privacy Commissioner v. Attorney General of Canada

This is an appeal to the Supreme Court of Canada of a decision of the Federal Court of Appeal. The issues are whether the Federal Court of Appeal erred in finding that the disclosure of "personal information" by Customs to the Canada Employment Insurance Commission was authorized by section 8 of the *Privacy Act* and section 108 of the *Customs Act,* whether paragraph 108(1)(b) of the *Customs Act* provides the Minister with authority to disclose personal information to the Commission for use in an investigative data match program, and whether the Minister properly authorized the disclosure of personal information in the Traveller Declaration Forms to the Commission for use in an investigative data match program.

This was a special case stated for opinion of the Federal Court jointly brought by my predecessor and the Attorney General of Canada. My predecessor was successful before the Federal Court Trial Division but unsuccessful before the Federal Court of Appeal.

The decision of the Federal Court of Appeal was delivered on February 9, 2000, from the bench. The main conclusions are as follows:

- The data match is authorized by the Ancillary Memorandum of Understanding for data capture and release of customs information on travellers entered into on April 26, 1997 by Customs and the Canada Employment Insurance Commission. Paragraph 108(1)(b) of the *Customs Act* gives the Minister of Revenue the discretionary power to authorize the arrangement set out in the 1997 Ancillary Memorandum. An earlier authorization issued in 1991 by the Minister of Revenue under paragraph 108(1)(b) of the *Customs Act* was determined not to be relevant to the matter before the court.
- Paragraph 8(2)(b) of the *Privacy Act* is to be interpreted broadly. The court stated: "In this context, paragraph 8(2)(b) cannot but be interpreted as being a provision that enables Parliament to confer on any Minister (for example) through a given statute a wide discretion, both as to form and substance, with respect to the disclosure of information his department has collected, such discretion, of course, to be exercised in conformity with the purpose of the *Privacy Act*."
- These objectives were met because "the Minister satisfied herself that the disclosure sought by the Commission was for a permissible use and that no more information than that needed by the Commission would be disclosed." In addition, the 1997 Ancillary Memorandum included restrictions on the use of the information and its disclosure to third parties and other measures such as the establishment of an audit trail and provision for destruction of information.

The Charter Challenge

This is an appeal to the Supreme Court of Canada of a decision of the Federal Court of Appeal. The issues are:

- Whether CCRA's disclosure to the Canada Employment and Insurance Commission of personal information from an individual's Traveller Declaration Form, the use of this information in a data match program, and its subsequent use as evidence against the individual, contravenes the individual's right to be secure from unreasonable search or seizure under section 8 of the Charter;
- If so, whether the evidence should have been excluded under subsection 24(2) of the Charter; and
- Whether the provision in the *Employment Insurance Act* which disentitles the individual from receiving benefits while outside of Canada infringes the applicant's mobility rights under subsection 6(1) of the Charter.

The application for judicial review of the decision of the Office of the Umpire appointed under the *Employment Insurance Act* was dismissed by the Federal Court of Appeal. The Federal Court of Appeal, in a decision delivered February 9, 2000, found that there is no reasonable expectation of privacy for Canadians in information contained in E-311 forms such as to engage section 8 of the Charter (right to be secure against unreasonable search and seizure). The court also decided that paragraph 32(b) of the *Unemployment Insurance Act* (now 37(b) of the *Employment Insurance Act:* no entitlement to Employment Insurance benefits while outside Canada) did not go against the freedom of movement guarantee under subsection 6(1) of the Charter.

Status

The applications for leave to appeal to the Supreme Court of Canada in both these cases were granted on August 17, 2000. Both Notices of Appeal were filed and served on August 22, 2000.

Notice of the Constitutional Questions in the Charter Challenge case was served on the Attorneys General of all the provinces and territories as required by the Supreme Court of Canada Rules. The Attorneys General of Ontario, Manitoba and Québec intervened.

These cases were heard on November 7, 2001.

Clayton Charles Ruby v. Solicitor General

This is an appeal to the Supreme Court of Canada of a decision of the Federal Court of Appeal. The applicant was denied access to his personal information in banks maintained by the Canadian Security Intelligence Service. The Solicitor General refused to release the information the applicant had requested. An application for review of the refusals was dismissed by the Federal Court Trial Division. The matter was appealed to the Federal Court of Appeal, where the appeal was allowed in part and two matters were remitted back to the Trial Division for new determination.

Both the Federal Court Trial Division and Federal Court of Appeal considered the constitutionality of section 51 of the *Privacy Act,* which provides for the filing of information *ex parte* with the court and that hearings be *in camera.* Both courts found that the section 2(b) Charter infringement caused by section 51 of the *Privacy Act* is justified under section 1 of the Charter. The issues in the Supreme Court are:

Issues in the Appeal

- Whether section 51 of the *Privacy Act* violates section 7 of the Charter; and if so, whether the violation is justified under section 1; and
- Whether the section 2(b) Charter infringement caused by section 51 of the *Privacy Act* is justified under section 1.

I*ssues in* C*ross-*A*ppeal*

- Whether the Federal Court of Appeal interpreted paragraph 22(1)(b) of the *Privacy Act* so narrowly that government institutions will not be able to adequately protect the names of sources of information including police informers; and
- Whether the Federal Court of Appeal failed to give adequate consideration to the implications of the "mosaic effect" and the necessity of interpreting the exempting provisions of the *Privacy Act* in such a manner as to preserve the government's ability to protect sources, investigative methods and techniques and the ability to effectively enforce the laws of Canada.

By decision dated June 8, 2000, the Federal Court of Appeal held that section 7 of the Charter was not engaged since the procedural safeguards in section 51 of the *Privacy Act* did not deprive individuals of their liberty interest. On section 2(b) of the Charter, the Federal Court of Appeal held that section 51 of the *Privacy Act* infringed the right to freedom of speech, but could be saved as a justifiable reasonable limit under section 1 of the Charter.

Another issue considered by the court was the proper interpretation of paragraph 22(1)(b) of the *Privacy Act* which permits a government institution to refuse access to personal information where the disclosure could reasonably be expected to be injurious to the enforcement of a law of Canada or a province or the conduct of lawful investigations. The Federal Court of Appeal rejected the argument of the Solicitor General and held that paragraph 22(1)(b) does not authorize a refusal to disclose simply because disclosure could have a chilling effect on the investigative process in general. The notion of injury in paragraph 22(1)(b) does not extend beyond injury to a specified investigation, either actual or to be undertaken.

S*tatus*

Mr. Ruby sought leave to appeal to the Supreme Court of Canada from the decision of the Federal Court of Appeal concerning the constitutionality of section 51 of the *Privacy Act.* The Solicitor General sought leave to cross-appeal from the decision of the Federal Court of Appeal regarding the interpretation of paragraph 22(1)(b) of the *Privacy Act.* Both applications for leave were granted by the Supreme Court of Canada on January 18, 2001. I applied for leave to intervene in the issue concerning paragraph 22(1)(b). I was granted leave to intervene on May 25, 2001. I will present arguments before the Supreme Court of Canada that differ from those of both parties.

Office of the Commissioner of Official Languages (Appellant) v. Robert Lavigne (Respondent)

This case is currently under appeal to the Supreme Court. Mr. Lavigne was refused access to his personal information 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 in paragraph 22(1)(b) of the *Privacy Act.*

Mr. Lavigne applied to the Federal Court Trial Division under section 41 of the *Privacy Act* for review of the Office's refusal. The previous Privacy Commissioner and I intervened in support of Mr. Lavigne throughout this litigation. Our interventions have been successful before both the Federal Court Trial Division and the Federal Court of Appeal.

By decision delivered September 6, 2000, from the bench, the Federal Court of Appeal ordered the Office of the Commissioner of Official Languages to provide Mr. Lavigne with his personal information. The Federal Court of Appeal relied on two of its previous decisions, *Rubin v. Canada (Minister of Transport)* and *Ruby v. Canada (Solicitor General),* confirming that the paragraph 22(1)(b) exemption can only be invoked where there is evidence of injury to a specific investigation, the exemption cannot be invoked once an investigation has been completed, and one cannot refuse to disclose the requested information on the basis that to disclose would have a "chilling" effect on possible future investigations. The Federal Court of Appeal rejected the argument of the Office of the Commissioner of Official Languages that a different interpretation was justified in this case by the statutory mandate of the Commissioner of Official Languages.

The issues in the Supreme Court are whether the Court of Appeal erred in finding that the access provisions of the *Privacy Act* override the confidentiality provisions of the *Official Languages Act* and whether the decision of the Court of Appeal seriously compromises the Commissioner of Official Languages' ability to enforce the *Official Languages Act.*

Status

The Office of the Commissioner of Official Languages filed an application for leave to appeal to the Supreme Court of Canada. Leave to appeal was granted on April 19, 2001. The Supreme Court of Canada granted me leave to intervene in support of Mr. Lavigne on August 21, 2001. My submissions as an intervener will be filed in early December.

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

Introduction

The passage of the *Personal Information Protection and Electronic Documents (PIPED) Act* is an important step forward for Canada. It is a clear commitment to protect our fundamental right of privacy, in an age when it is threatened as never before. With technological developments revolutionizing the way we do business and with organizations demonstrating a limitless appetite for personal information, progressive nations around the globe are recognizing the need to safeguard privacy. The *PIPED Act* places Canada firmly in their front ranks.

Part 1 of the *Act* sets out the conditions under which organizations may collect, use, or disclose personal information, and gives individuals rights of access to and correction of personal information held about them by an organization. It also sets out the process by which individuals may lodge a formal complaint when they believe these rights have been violated or that organizations are not in compliance with the law, and the legal remedies available to them.

This part of the *Act* is being implemented in three stages. In the first stage, which began on January 1, 2001, the *Act* applies to personal information, except personal health information, collected, used or disclosed in the course of commercial activities, or about their

employees, by federal works, undertakings and businesses. This includes the banks, the broadcasting industry, inter-provincial transportation companies and the telephone companies.

The *Act* also applies to disclosures of personal information traded or sold across provincial or national borders. In addition, it applies to the entire commercial sector in the Yukon, Northwest Territories and Nunavut, since all local businesses in the territories are considered to be federal works, undertakings, and businesses, and therefore under the jurisdiction of the federal Parliament.

As of January 1, 2002, the *Act* will apply to personal health information for the organizations and activities already covered in the first stage.

Part 1 of the *Act* will be in force across Canada in the provincially regulated private sector as of January 1, 2004, except where a province or territory has enacted legislation that the Governor in Council considers to be substantially similar to the *Personal Information Protection and Electronic Documents Act.* In these cases, the provincial or territorial legislation will apply to intra-provincial collection, use or disclosure of personal information by organizations subject to the provincial law. The federal law will continue to apply to a broad range of interprovincial and international collections, uses or disclosures. That means that as of January 1, 2004, the privacy rights of Canadians will be protected throughout the private sector, either under the federal *Act* or under a substantially similar provincial or territorial law.

As Privacy Commissioner of Canada, I am responsible for overseeing compliance with the rules for the collection, use, and disclosure of personal information set out in Part 1 of the *Act*. I receive and investigate complaints, and, as with the *Privacy Act,* play the role of an ombudsman, attempting to resolve disputes by negotiation. I also may, with reasonable grounds, audit the personal information management practices of an organization.

The powers of investigation granted to my Office under the *Personal Information Protection and Electronic Documents Act* mirror those contained in the *Privacy Act,* although I have a greatly expanded mandate to conduct research into privacy issues, and to promote awareness and understanding of these issues among Canadians.

This is an interim report on activities related to the *Personal Information Protection and Electronic Documents Act* covering the period from January 1, 2001, to November 30, 2001.

Update on Provincial and Territorial Legislation

Determination of "Substantially Similar"

I will interpret substantially similar as meaning equal or superior to the federal law in the degree and quality of privacy protection provided. The federal law is the threshold or floor. A provincial privacy law must be at least as good, or it is not substantially similar.

To be considered substantially similar, any provincial legislation will have to contain, at a minimum, the 10 principles set forth in Schedule 1 to the *Personal Information Protection and Electronic Documents Act.* While we consider all 10 principles of this code to be interrelated and equally important, I am going to comment on five elements of the law as key components in making an assessment of substantially similar: consent, reasonable person test, access and correction rights, oversight, and redress.

Consent

To the extent that privacy is the right to control access to one's person and to personal information about oneself, there is no control without consent and there is no privacy without control.

The requirement for consent must be at the heart of any good privacy legislation. The federal law says that consent must be informed and that the collection, use and disclosure of personal information without the individual's consent may occur only in specified exceptional circumstances.

An organization can only collect, use or disclose personal information about an individual with the individual's consent (except in certain limited circumstances that are set out in the *Act.*)

After collection, personal information can only be used or disclosed for the purpose for which consent was given (except in certain circumstances that are set out in the *Act.*)

Reasonable Person Test

The reasonable person test provides another important check on organizations. The law states that the collection, use, and disclosure of personal information must be limited to purposes that a reasonable person would consider appropriate in the circumstances.

Among other things, this test prevents organizations from using overly broad or vague statements of the purposes for which information is being collected.

Access and Correction Rights

Individuals must have the right to access personal information that organizations have about them and to correct any information that is incorrect (or to have any disagreement noted and provided to any party who received the information).

Oversight

Where an individual is of the opinion that his or her privacy rights have been violated or the privacy law not respected, the individual must have the ability to complain to a fully independent oversight body with the specific mandate to resolve complaints, thoroughly investigate, mediate, conciliate and make recommendations or issue orders. Such an oversight body also must have the full range of investigative powers to seize documents, enter premises, and compel testimony and initiate audits of an organization's practices.

Redress

Following my report to an organization and a complaint, the federal *Act* allows the complainant (or myself directly) to apply for a hearing in the Federal Court of Canada. The complainant or I can ask the court to order the organization in question to correct its information handling practices and make public the steps it has taken to do so. The court can be asked to award damages to the complainant.

Decisions of the Federal Court can be appealed to the Federal Court of Appeal and with leave to the Supreme Court of Canada.

I believe that there must be corresponding redress provisions in any provincial legislation which purports to be "substantially similar".

Legislative initiatives to regulate the private sector

To date, Quebec is the only province in Canada with personal data protection in effect that applies to enterprises operating in the province as defined in its Civil Code. Elsewhere in Canada, two provincial governments – British Columbia and Ontario – have begun to explore legislative options for the regulation of the collection, use, and disclosure of personal information in the private sector. This is in preparation for the January 1, 2004, date for provincial governments to have legislation in place that is deemed by the Governor in Council, through an exemption order, to be substantially similar to the *Personal Information Protection and Electronic Documents Act.*

Health Sector

The provinces of Alberta, Manitoba and Saskatchewan have all passed health-specific privacy legislation. The legislation in Manitoba and Alberta is currently in force. In December 2000, Ontario introduced the controversial Bill 159, the *Personal Health Information Privacy Act.* This bill died on the order paper.

Public Sector Legislation

New Brunswick's *Protection of Personal Information Act* came into force in April 2001. Prince Edward Island's *Freedom of Information and Protection of Privacy Act* received Royal Assent on May 15, 2001, and will come into force in November 2002. With the introduction and passage of these two acts, every province and territory in Canada with the exception of Newfoundland now has statutory protection for personal information held by government departments and agencies.

Investigations

As of November 30, 2001, my Office had received 95 formal complaints under the *Personal Information Protection and Electronic Documents Act.* During this first year of the *Act*, these complaints have been confined to the federally regulated sector, with nearly half of them involving the banks.

In spite of the lead-in time organizations had to prepare for the coming into force of the *Act*, some still have not embraced its principles in their business practices. Many complaints have raised systemic issues dealing with the violation of privacy rights in the federally regulated private sector. Where it was determined that they were well-founded, I have recommended that organizations make important changes to existing policies and procedures.

Section 13 of the *Personal Information Protection and Electronic Documents Act* gives me the authority to ask that organizations report back on the progress made in implementing these changes. Experience to date suggests that this will be a useful tool to ensure the necessary changes are made.

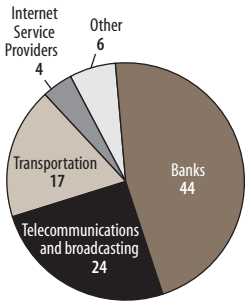
My approach to the investigation and resolution of these complaints is similar to my approach under the *Privacy Act.* When my Office receives a complaint, I give the organization formal notice of the nature of the allegations, and invite it to make representations. I try, whenever possible, to resolve disputes through conciliation, consultation, persuasion and mediation.

I may make one of the following findings in handling a complaint:

- **Not well-founded:** This means that there is no evidence to lead me to conclude that the organization violated the *Act*.
- **Well-founded:** This means that the investigation revealed that the organization failed to respect a provision of the *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 my Office's inquiries.
- **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.

Complaints by Sector

January 1, 2001 to November 30, 2001



Commissioner's Findings

The following are my findings under the *PIPED Act* up until November 30, 2001. For the sake of consistency, the findings are presented in the format in which they will appear on our Web site at **www.privcom.gc.ca.** Since January 2001 my Office has completed investigations and issued findings and recommendations in the investigation of 27 complaints under the *Personal Information Protection and Electronic Documents Act* and two incidents. Complaints almost identical in nature have been combined and written as one finding.

Video surveillance activities in a public place [Principle 4.3, Schedule 1]

Complaint

The Information and Privacy Commissioner of the Northwest Territories and Nunavut complained that a security company had improperly collected personal information without the consent of individuals by means of surveillance cameras installed on the main street of Yellowknife.

Summary of Investigation

The security company in question had mounted, on the roof of its office building, four video cameras aimed down into a main intersection of Yellowknife and had set up two monitors in its offices. For several days in early May 2001, company staff had monitored live feed from the street 24 hours a day. On several occasions, staff had noted incidents and contacted police. By the company's own admission, this surveillance activity had been a marketing demonstration intended to generate business. On negative publicity, the company removed the cameras less than a week after they had been installed.

Commissioner's Findings (Issued June 15, 2001)

Jurisdiction: As of January 1, 2001, the *Personal Information Protection and Electronic Documents Act* applies to federal works, undertakings, or businesses. The Commissioner had jurisdiction in this case because any company in the Northwest Territories is a federal work, undertaking, or business as defined in the *Act*.

Application: Principle 4.3, Schedule 1, states that the knowledge and consent of the individual are required for the collection, use, or disclosure of personal information, except where inappropriate.

Since the company's principal reason for installing video surveillance equipment was to monitor the activities of people, the Commissioner concluded that the information at issue was personal information for purposes of the *Act*. Since the company had admitted that its video surveillance activity was a marketing demonstration, the Commissioner concluded that the activity was a commercial activity within the meaning of the *Act*.

The fact that the video feed was live and not taped, was deemed not relevant, since the *Act* does not restrict personal information to recorded information. On the evidence, the Commissioner was satisfied that individuals had not consented to the collection. He found that the company had collected personal information without consent in contravention of Principle 4.3.

In presenting his findings, the Commissioner commented as follows: "There may be instances where it is appropriate for public places to be monitored for public safety reasons. But this must be limited to instances where there is a demonstrable need. It must be done only by lawful public authorities and it must be done only in ways that incorporate all privacy safeguards set out by law. There is no place in our society for unauthorized surveillance of public places by private sector organizations for commercial reasons."

The Commissioner concluded therefore that the complaint was well-founded.

Further Considerations

No further action was required in respect of the complaint, since the company had already removed the cameras before the Commissioner issued his findings. However, the matter was not fully resolved, in that the security company indicated an intention to pursue its efforts to provide video surveillance services to the Yellowknife community. The Commissioner has advised the company that its intended public video surveillance for commercial purposes is unlawful and should not be pursued.

Unsolicited e-mail from an Internet service provider [Principle 4.3, Schedule 1]

Complaint

A customer complained that her Internet service provider (ISP) was using her personal information, namely her e-mail address, without her consent by sending unsolicited e-mail notices to her.

Summary of Investigation

The complainant had received several unsolicited e-mail notices from her ISP about its services. At first she complained directly to the ISP, but was not satisfied with the company's suggestion that she simply reconfigure her browser so as to route the notices directly to a bulk-mail or trash-bin folder. Her position was that the onus should not be on the user to filter unsolicited e-mail notices from the ISP. The company's position was that it had a right to send such messages under the terms and conditions of its subscriber agreement, which contains a consent clause.

Since the initial one-year subscription had been a gift from a friend, the complainant had not personally considered these terms and conditions at the start of her service, but had subsequently been presented with them on renewing her subscription after a year. The complainant did renew her subscription with the same company even though her complaint remained unresolved at the time.

Commissioner's Findings (Issued July 3, 2001)

Jurisdiction: As of January 1, 2001, the *Personal Information Protection and Electronic Documents Act* applies to federal works, undertakings, or businesses. The Commissioner had jurisdiction in this case because Internet service providers are federal works, undertakings, or businesses, as defined in the *Act*.

Application: Principle 4.3, Schedule 1, states that the knowledge and consent of the individual are required for the collection, use, or disclosure of personal information, except where inappropriate.

On reviewing the subscriber agreement of the ISP in question, the Commissioner was satisfied that the company's practice of sending periodic e-mail notices to customers was clearly outlined in the agreement. Hence, he considered it reasonable that customers would expect to receive such notices from time to time. Moreover, he determined that the complainant had consented to the practice on renewing her subscription. He found that in this case the ISP had not contravened Principle 4.3.

The Commissioner concluded therefore that the complaint was not well-founded.

Further Considerations

The Commissioner informed the complainant that he considered the ISP's initial proposal for resolving her concern to have been reasonable. He also commented: "The e-mail notices are in keeping with the purposes for which consent to use the e-mail address was originally obtained, that is, to enable efficient ISP service."

Commissioner considers jurisdiction over third-party disclosure by bank subsidiary [Section 30]

Complaint

A customer complained that an investment company, a subsidiary of a chartered bank, had improperly disclosed to a third party, namely a regulatory body that oversees the company's activities, his personal information related to financial transactions.

Summary of Investigation

The investigation in this case was limited to the Commissioner's determination of whether or not he had jurisdiction in the matter.

Commissioner's Findings (Issued July 19, 2001)

Jurisdiction: As of January 1, 2001, the *Personal Information Protection and Electronic Documents Act* applies strictly to federal works, undertakings, or businesses and to transborder disclosures of personal information for consideration. Banks are federal works, undertakings, or businesses as defined in the *Act*. In this case, however, the investment company, though a subsidiary of a bank, operates as a separate and distinct legal entity, does not disclose information across borders for consideration, and is provincially

regulated. The company in question is not currently subject to the *Act*.

The Commissioner concluded that he lacked jurisdiction.

Bank customer requests credit score information [Principle 4.9, Schedule 1, and section 8]

Complaint

A customer complained that a bank had denied her access to her personal information regarding her credit score.

Summary of Investigation

The complainant had telephoned her branch of the bank in question and asked for her credit score information. A customer service representative at the branch advised her that the bank did not release such information to its customers. On being informed of this complaint, the bank undertook an extensive search of its records and subsequently reported that it could not find any credit product or credit application in the complainant's name and therefore had no corresponding credit score for her. The complainant subsequently confirmed that she had no credit products with the bank and had never submitted any credit application to the bank.

Commissioner's Findings (Issued July 23, 2001)

Jurisdiction: As of January 1, 2001, the *Personal Information Protection and Electronic Documents Act* applies to federal works, undertakings, or businesses. The Commissioner had jurisdiction in this case because financial institutions are federal works, undertakings, or businesses as defined in the *Act*.

Application: Principle 4.9, Schedule 1, states that upon request an individual must be informed of the existence, use, and disclosure of his or her personal information and be given access to that information. Section 8 sets out conditions under which a request may be deemed to have been refused.

The Commissioner was satisfied that the requested information did not exist in the bank's files. He found therefore that the complainant had not been denied a right of access to her personal information under section 8 of the *Act*.

The Commissioner concluded that the complaint was not well-founded.

Personal information retained after application rejected [Principle 4.5, Schedule 1]

Complaint

A credit card applicant complained that, after turning down her application, a bank had refused her request that the personal information collected for her application be deleted from the bank's records.

Summary of Investigation

The complainant had applied in person for a credit card, but the bank in question had declined her application. The complainant then requested that the personal information

she had provided in her application be removed from the bank's computer system. The branch manager replied that he himself did not have the delegated authority to remove the information, and he took no steps to determine whether some other course could be taken.

In fact, the bank's corporate privacy officer and the business manager for the credit cards had the delegated authority for removal of such information on special request, but in this case the complainant's request was not relayed to either of these officials. For credit card applications made in person, the bank's usual practice was to enter the personal information collected immediately into the computer system at the branch and then forward it for adjudication to the host computer system of the bank's central loan processing centre. If the application was declined, the information was not automatically purged. Unless the unsuccessful applicant made a special request for removal, the personal information remained in the bank's computer system and was accessible indefinitely at the branch level.

Commissioner's Findings (Issued July 23, 2001)

Jurisdiction: As of January 1, 2001, the *Personal Information Protection and Electronic Documents Act* applies to federal works, undertakings, or businesses. The Commissioner had jurisdiction in this case because banks are federal works, undertakings, or businesses, as defined in the *Act*.

Application: Principle 4.5, Schedule 1, states that personal information must be retained only as long as necessary for the fulfillment of the purposes for which it was collected.

The Commissioner considered it unreasonable that, after the bank had used the complainant's personal information for the purpose for which it had been collected (i.e., making the decision about the credit card), the information would have remained accessible indefinitely at the branch level had the complainant not insisted on its removal. He found that the bank in this case had contravened Principle 4.5.

However, the Commissioner also noted that the bank had subsequently deleted the complainant's personal information and had confirmed that it had not been communicated to any third party. He also noted that the complainant was satisfied with this resolution.

The Commissioner concluded therefore that the complaint was well-founded and resolved.

Further Considerations

To address the inconsistencies revealed by the Commissioner's investigation, the bank in question has agreed to undertake an extensive review of its current practices for the retention of personal information. The bank has also agreed to implement a communications strategy for educating employees and customers on the bank's privacy complaints process.

Security of a bank's automated telephone service [Principle 4.7, Schedule 1]

Complaint

Citing several provisions of the *Personal Information Protection and Electronic Documents Act,* an individual complained that a bank was not taking adequate security measures to safeguard customers' information disclosed via its automated telephone service.

Summary of Investigation

The bank in question offers an automated telephone service for Visa customers who do not have other dealings with the bank. Users of this service cannot conduct transactions, but can gain limited access to their Visa account information by providing the 16-digit Visa account number and, at the random selection of the system, either the last four digits of the cardholder's home telephone number or the cardholder's year of birth.

Commissioner's Findings (Issued July 23, 2001)

Jurisdiction: As of January 1, 2001, the *Personal Information Protection and Electronic Documents Act* applies to federal works, undertakings, or businesses. The Commissioner had jurisdiction in this case because banks are federal works, undertakings, or businesses, as defined in the *Act*.

Application: Principle 4.7, Schedule 1, states that an organization must protect personal information by security safeguards appropriate to the sensitivity of the information.

On consideration, the Commissioner deemed the complainant's concern to be valid. He determined that a coding procedure relying so much upon a cardholder's telephone number or year of birth was not adequate to prevent unauthorized persons from gaining access to users' sensitive personal information. He found that the bank in question was not in compliance with Principle 4.7.

Nevertheless, the Commissioner noted that the bank had proposed and initiated a detailed three-phase action plan to address the security concerns raised in the complaint. He also noted both he and the complainant found all aspects of this plan satisfactory.

The Commissioner concluded therefore that the complaint was well-founded and resolved.

Further Considerations

The action plan proposed by the bank comprises three-phases as follows:

Immediate: All automated access to the complainant's Visa account is disabled, so that any unauthorized attempt to obtain the complainant's personal information will fail. The complainant himself will be able to access his account through an agent by reference to a preselected password.

Short-term: By October 31, 2001, the bank's Visa-only customers will be allowed to disable their automated telephone access upon request and likewise deal directly with an

agent, if they so choose. This phase includes a communications strategy for informing the customers.

Long-term: The bank has agreed to implement a new telephone bank solution addressing the privacy and security concerns of customers within three years and to report on progress to the Privacy Commissioner no later than July 31, 2002.

The Commissioner has commented: "I am satisfied that the measures [the bank] has put in place to resolve the security safeguard issues identified … are acceptable."

Musician objects to collection of salary information by professional organization [Section 2]

Complaint

A musician complained that the professional organization representing his interests had, without his consent, collected personal information about him, namely his annual salary, from his employer.

Summary of Investigation

The complainant is the only musician working in a certain establishment. One of the activities of the professional organization in question is to collect copyright dues for its members, subject to the requirements of the *Copyright Act.* In order to file the applicable tariff with the Copyright Board and collect the copyright dues, the organization first needs to know the total entertainment budget of a given establishment. The complainant was concerned that, since he was the only musician at the establishment in question, a third-party might be able to identify him as the sole recipient of the salary allotment included in the entertainment budget. However, in collecting such information, the organization has no interest in knowing which musicians or how many are working in the establishment and therefore does not collect names or numbers. Nor does it publish or communicate to third parties the information it collects in respect of the establishment.

Commissioner's Findings (Issued July 23, 2001)

Jurisdiction: The professional organization in question stated that it was subject to the *Personal Information Protection and Electronic Documents Act.* The Commissioner did not dispute this position.

Application: Section 2 of the *Act* defines personal information to be "… information about an identifiable individual …".

On the evidence, the Commissioner was satisfied that the professional organization had the legal authority to collect the information at issue and that the collection did not involve personal information about an identifiable individual. He found that the collection was therefore not subject to the requirements of the *Act*.

The Commissioner concluded that the complaint was not well-founded.

Further Considerations

In conveying his findings, the Commissioner commented: "Having established that the information collected is not personal, I need not make a finding on its appropriateness with respect to sections 4.3 (consent) and 4.4 (limiting collection) of Schedule 1 or to section 7 (collection without knowledge or consent) of the *Act*, which might otherwise have applied in this case."

Use and disclosure of personal information in telephone directories [Principle 4.3, Schedule 1]

Complaint

Citing several provisions of the *Personal Information Protection and Electronic Documents Act,* an individual complained that a telecommunications company was:

1. Using and disclosing customers' personal information without their knowledge and consent by publishing names, addresses, and telephone numbers in the company's white-pages directory and on two Web sites; and

2. Inappropriately charging customers for opting not to have their information published.

Summary of Investigation

The telecommunications company in question publishes customers' names, addresses, and telephone numbers in its white-pages directory and on its own directory assistance Web site.

In accordance with Canadian Radio-television and Telecommunications Commission (CRTC) regulations, the company gives the same information to the Bell Canada subsidiary that operates the "Canada 411" Web site. Customers are asked how they wish their personal information to appear in the company's white pages and are given the option of not having their information published. For those who choose non-publication, the company charges fees, in accordance with CRTC regulations. The company also provides list services to selected organizations for a fee, excluding information on non-published customers and customers who ask to be de-listed.

Commissioner's Findings (Issued August 14, 2001)

Jurisdiction: As of January 1, 2001, the *Personal Information Protection and Electronic Documents Act* applies to federal works, undertakings, or businesses. The Commissioner had jurisdiction in this case because telecommunications companies are considered to be federal works, undertakings, or businesses, as defined in the *Act*.

Application: Principle 4.3, Schedule 1, states that the knowledge and consent of the individual are required for the collection, use, or disclosure of personal information, except where inappropriate.

On the matter of consent, the Commissioner considered relevant the company's questioning of customers regarding how their information should appear in the white-pages directory.

He determined that the question itself implies the eventual appearance of the information in publicly available directories. By choosing not to take the option of non-publication, customers implicitly give consent for their personal information to be made available to the public. Moreover, since the information subsequently published in other formats merely reflects what is published in the white-pages directory, it too is considered publicly available information for purposes of the regulations under the *Act* and may be collected, used, or disclosed without consent. In sum, the Commissioner found that the company did obtain valid consent and was in compliance with regulations on publicly available information.

On the matter of charging fees for non-publication of customers' information, the Commissioner noted that the company had duly applied for and received permission from the CRTC, under Telecom Order 98-109, which states that telecommunications companies can charge no more than $2 per month for non-published telephone service. He founded therefore that the company in question did have authority to charge its monthly fee of $2 for non-publication.

The Commissioner concluded that the complaint was not well-founded.

Bank teller writes account number on cheque [Section 5(3)]

Complaint

An individual complained that a bank had created the potential for an improper disclosure of his personal information to a third-party without his consent when a teller wrote his account number on the back of a cheque when cashing it.

Summary of Investigation

The complainant had gone to a branch of his bank to cash a personal cheque from a third party. The bank teller wrote the complainant's account number on the back of the cheque. The complainant's concern was that, if the cheque was for any reason returned to the third party who had written it, the account number would be disclosed to that person.

The bank argued that, in cashing cheques, banks are in effect extending credit until such time as the cheque's value can be debited from the cheque-writer's account. In cases of exception (e.g., fraud or insufficient funds), banks require an efficient means of recovering the cheque value from the customer who presented the cheque. Moreover, names written on the front of cheques are not an efficient enough means, in that they may vary significantly from the exact names in which customers' bank accounts are registered. This bank's position was that recording account numbers on cheques is a longstanding industry-wide practice, necessary for protecting

a bank's interests in ensuring that it can collect its money from either the cheque-writer or the person who deposits or cashes the cheque.

Commissioner's Findings (Issued August 14, 2001)

Jurisdiction: As of January 1, 2001, the *Personal Information Protection and Electronic Documents Act* applies to federal works, undertakings, or businesses. The Commissioner had jurisdiction in this case because banks are federal works, undertakings, or businesses as defined in the *Act*.

Application: Section 5(3) states that an organization may collect, use or disclose personal information only for purposes that a reasonable person would consider are appropriate in the circumstances.

The Commissioner determined that the bank's recording of the account number at the time a cheque is presented is a reasonable practice and that it is reasonable for a customer to expect such practice. The Commissioner was satisfied that the complainant had thus given implied consent to the collection, use, and disclosure of his personal information. The Commissioner found that no contravention of the *Act* had been established.

He concluded therefore that the complaint was not well-founded.

Further Considerations

In presenting his findings, the Commissioner commented as follows: "Upon presenting the cheque for negotiation, the [bank's] customer is giving implied consent for the disclosure of the personal information on the back, just as the drawee is providing express consent to disclosure of their personal information (on the front of the cheque) to the payee."

Trucking company collects personal information intended for Canada Customs [Principle 4.4, Schedule 1]

Complaint

A dismissed employee complained that his former employer, an international trucking company, had improperly attempted to collect personal information by insisting that he complete and return to the company an application for a program instituted by the Canada Customs and Revenue Agency (CCRA).

Summary of Investigation

The trucking company in question had sent the complainant, one of its international drivers, a letter advising that he was required to complete a "Commercial Driver Registration Application" under the new Customs Self-Assessment Program instituted by the CCRA. This letter also advised that the driver was to return the completed application to the company itself. The complainant refused, not wishing his employer to have access to the personal information he was required to provide on the application. The company sent

him a second letter ordering him to complete and return the application by a given date or else be disciplined under the collective agreement and have his employment placed in jeopardy. The complainant again did not comply, and the company terminated his employment five days after the given date. According to the company, the CCRA expected employers to gather applications and submit them to the CCRA on their drivers' behalf. In fact, the CCRA clearly instructs, on both the application form and the program pamphlet, that drivers submit their completed applications directly to the CCRA's processing centre in Niagara Falls.

Commissioner's Findings (Issued August 17, 2001)

Jurisdiction: As of January 1, 2001, the *Personal Information Protection and Electronic Documents Act* applies to federal works, undertakings, or businesses. The Commissioner had jurisdiction in this case because interprovincial trucking companies are federal works, undertakings, or businesses as defined in the *Act*.

Application: Principle 4.4, Schedule 1, states that collection of personal information must be limited to that which is necessary for the purposes identified by the organization and that information must be collected by fair and lawful means.

The Commissioner determined that, although it was necessary for a driver to complete an application for the Customs Self-Assessment Program and return it to the CCRA, it was not necessary or appropriate for the company itself to collect the information. He also determined that threatening employees with loss of their jobs was not a fair means of collection. He found that the company was not in compliance with Principle 4.4.

The Commissioner noted that the company had been prompt in changing its policy so as no longer to require its drivers to return their applications to the company. Nevertheless, he did not consider the complaint to have been resolved, pending reinstatement of the complainant with the company and compensation for any damages. The Commissioner expressed his intention to pursue these matters with the company.

The Commissioner concluded that the complaint was well-founded.

Further Considerations

The complainant subsequently informed the Commissioner that a settlement regarding the termination of his employment had been reached through arbitration and that he considered the complaint to have thus been satisfactorily resolved.

Bank loses customer's personal information [Principle 4.7, Schedule 1, and section 12(2)]

Complaint

A customer complained that a bank had failed to protect her personal information when documents containing her Social Insurance Number (SIN), name, address and unlisted telephone number were lost during a transfer between offices.

Summary of Investigation

Human Resources Development Canada had issued the complainant a new SIN after her discovery that her old one had been used fraudulently. She later completed forms that her bank required for updating her investment account information with the new SIN. She gave the completed forms to staff at a local branch office of the bank for transfer to the office of the subsidiary that manages the investment account. The documents were lost during the transfer.

Commissioner's Findings (Issued September 7, 2001)

Jurisdiction: As of January 1, 2001, the *Personal Information Protection and Electronic Documents Act* applies to federal works, undertakings, or businesses. The Commissioner had jurisdiction in this case because banks are federal works, undertakings, or businesses as defined in the *Act*.

Application: Principle 4.7, Schedule 1, states that personal information must be protected by security safeguards appropriate to the sensitivity of the information. Section 12(2) states that the Commissioner may attempt to resolve complaints by means of dispute resolution mechanisms such as mediation and conciliation.

At the outset of the Commissioner's investigation, the parties indicated an interest in resolving the matter. Discussions ensued, and a settlement satisfactory to both parties eventually resulted. Furthermore, the Commissioner was satisfied that the bank in question had taken steps to ensure that appropriate safeguard policies, practices, and procedures were in place.

The Commissioner concluded therefore that the complaint was resolved and no further action necessary.

Further Considerations

Both the complainant and the bank expressed satisfaction with the role that the Commissioner's Office had assumed in settling this matter.

Credit card applicant objects to bank's information-sharing policy

Complaint

An individual complained that a bank was refusing to process his credit card application because he would not consent to the bank's information-sharing policy.

Summary of Investigation

In filling out an application for a credit card, the complainant had marked up the terms and conditions by hand. His intention in doing so had been to indicate his disagreement with the bank's stated policy of sharing personal information and to exercise the option of not having his personal information shared and not receiving the bank's direct marketing service. The bank subsequently advised him by letter that it was unable to process his application as submitted because the legal wording had been amended. The complainant interpreted this letter as being a refusal on the bank's part to issue a credit card unless he authorized its information-sharing policy. In a second letter, the bank assured the complainant that applicants did have the right to opt out of the direct-marketing service and that his own application had been returned to him simply because he had altered it. The bank also offered to reconsider his credit card application and at the same time to remove his name from its direct-marketing and shared-marketing lists. The complainant agreed.

On being finally issued a credit card, the complainant pronounced himself satisfied with the bank's response and indicated that his complaint file the Office could be closed.

Accordingly, this complaint was discontinued.

Bank accused of withholding bond certificates [Principle 4.9, Schedule 1; and section 8]

Complaint

An individual complained that a bank had denied her access to her personal information in the form of two "Small Business Bonds" that she believed the bank was holding under her name.

Summary of Investigation

The complainant specified that the documents she was seeking were the paper versions or certificates of two "Small Business Bonds". In 1982, the complainant and her spouse had consolidated their outstanding indebtedness to the bank in question under the Small Business Bond (SBB) Program, a federal government initiative that provided interest relief for borrowers. The bank had advised the complainant as early as 1984 that "Small Business Bond" was only a term used and that the only actual document signed in respect of the SBB Program was a form entitled "Election in Respect of an SBB". Both the bank and Industry Canada have confirmed that this form was the only document directly related to the program; no actual paper versions or certificates of SBBs had ever existed. In 1998,

during a lawsuit over the complainant's defaulting on her loan agreement, the bank had been obliged to disclose to the complainant and her lawyer all documents it held in relation to her involvement in the SBB Program. The complainant received her signed "Election in Respect of an SBB" form at that time and was still in possession of it when she filed her complaint with the Office.

Commissioner's Findings (Issued September 18, 2001)

Jurisdiction: As of January 1, 2001, the *Personal Information Protection and Electronic Documents Act* applies to federal works, undertakings, or businesses. The Commissioner had jurisdiction in this case because banks are federal works, undertakings, or businesses as defined in the *Act*.

Application: Principle 4.9, Schedule 1, states that upon request an individual must be informed of the existence, use, and disclosure of his or her personal information and be given access to that information. Section 8 sets out conditions under which a request may be deemed to have been refused.

The Commissioner found no evidence of the existence of SBB-related documents other than those already received by the complainant. Satisfied that the documents sought by the complainant did not exist, he found that the bank had not refused the complainant a right of access.

The Commissioner concluded therefore that the complaint was not well-founded.

Selling of information on physicians' prescribing patterns [Sections 2 and 3]

Two Complaints

In two separate complaints an individual and a physician complained that the Canadian arm of a U.S.-based international marketing firm was improperly disclosing personal information by gathering and selling data on physicians' prescribing patterns without their consent.

Summary of Investigation

The marketing firm in question gathers, from pharmacies and other Canadian sources, information related to medical prescriptions. The accumulated information includes names, identification numbers, telephone numbers, and prescribing details of physicians. This information is transferred to the firm's processing centre in the U.S., where the firm produces customized information products. These products typically identify physicians in a given territory and rank them, either individually or in groups, by monthly prescribing activity for various types or classes of drugs. The information products are then transferred to the firm's Montreal operation, where they are disclosed to clients for a fee. Pharmaceutical sales representatives from several Canadian provinces regularly buy these products.

Commissioner's Findings
(Issued September 21, 2001)

Jurisdiction: As of January 1, 2001, the *Personal Information Protection and Electronic Documents Act* applies to any information disclosed outside a province for consideration. Since the information at issue was regularly transmitted across borders, the Commissioner determined that it was information disclosed outside a province for consideration and therefore that he was required to receive and investigate the complaint.

Application: Section 2 of the *Act* defines personal information as "information about an identifiable individual, but does not include the name, title or business address or telephone number of an employee of an organization." Section 3 of the *Act* sets out the *Act*'s 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.

The primary consideration for the Commissioner was whether the information at issue was personal information within the meaning, scope, and purpose of the *Act*. In making this determination, the Commissioner took the view that the meaning of "personal information", though broad, is not so broad as to encompass all information associated with an individual. An individual prescription, though potentially revealing about a patient, 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 be regarded as a work product – that is, the tangible result of the physician's work activity.

The Commissioner determined that interpreting "personal information" so broadly as to include prescriptions or prescribing patterns would not fulfil the purpose set out in section 3 of the *Act* (see above). Specifically, it would not be reasonable to extend the definition to prescriptions, lest it be extended also to other work products such as legal opinions or documents written in the course of employment. Nor would it be reasonable to extend the definition to prescribing patterns, lest it be extended also to patterns discoverable among other types of work products and thus preclude many kinds of legitimate commercial consumer reporting.

In sum, the Commissioner found that prescription information, whether in the form of an individual prescription or in the form of patterns discerned from many prescriptions, is not personal information about a physician.

The Commissioner concluded therefore that the complaints were not well-founded.

Further Considerations

Because of widespread public interest in the case, the Commissioner published his letter of findings as a press release, dated October 2, 2001.

Estate executor disappointed in search for safety deposit box information [Principles 4.5, 4.9, Schedule 1; and section 8(7)]

Complaint

An estate executor complained that a bank had refused his request for personal information relating to the safety deposit box of his deceased aunt.

Summary of Investigation

The complainant suspected that a certain unauthorized person had, with help from the estate's lawyers, gained access to the deceased aunt's safety deposit box and removed items of value. The complainant had obtained a piece of evidence (i.e., a negative reply by fax from one branch of the bank) strongly suggesting that the bank had received at least one independent inquiry from the lawyers concerning the bank holdings of the deceased. In his capacity as estate executor, the complainant asked the bank for access to the signature card for the safety deposit box and to any correspondence between the bank and the estate's lawyers. The bank responded that it could locate neither the card nor any such correspondence. An exhaustive search of the bank files, involving the bank's own ombudsman, the Canadian Banking Ombudsman, and the Office of the Privacy Commissioner, proved unsuccessful in locating any of the information sought by the complainant.

Normally, the bank keeps safety deposit box signature cards for seven years. All the safety deposit boxes had been transferred from one branch of the bank to another eight days after the aunt's death, but appropriate security measures had been taken during the transfer. It was not bank policy for a branch to keep records of an account, an investment, or a safety deposit box once transferred to another branch. Nor was it bank policy for a branch to keep requests for information pertaining to a file it no longer held.

Commissioner's Findings (Issued October 12, 2001)

Jurisdiction: As of January 1, 2001, the *Personal Information Protection and Electronic Documents Act* applies to federal works, undertakings, or businesses. The Commissioner had jurisdiction in this case because banks are federal works, undertakings, or businesses as defined in the *Act*.

Application: Principle 4.9, Schedule 1, states that upon request, an individual shall be informed of the existence, use, and disclosure of his or her personal information and shall be given access to that information. Section 8(7) states that an organization that responds within the time limit and refuses a request shall inform the individual in writing of the refusal, setting out the reasons and any recourse that they may have under this part.

The Commissioner determined that the information the bank could not produce should have been retained in accordance with Principle 4.5 or should not have been lost.

He therefore found that the bank had not complied with Principle 4.9. He also found that the bank's response constituted a refusal under section 8(7).

The Commissioner concluded therefore that the complaint was well-founded.

Further Considerations

The Commissioner recommended that the bank revise its practices concerning the destruction of documents containing personal information and develop a written policy on the retention of such documents in conformance with the relevant provisions of the *Act*.

Employee alleges non-consensual disclosure by employer to investment firm [Section 7(3) and Principles 4.3 and 4.5, Schedule 1]

Complaint

An employee of a large corporation complained that his employer was improperly disclosing his and other employees' personal information, including information related to cash bonuses, without the employees' consent or prior knowledge, to the investment firm involved in an RRSP and savings plan sponsored by the corporation.

Summary of Investigation

The corporation in question has admitted that it discloses employees' personal information without their explicit consent to the investment firm involved in its RRSP and savings plan for hourly employees. The information disclosed consists of the individual's payroll and personal identification numbers, name, address, social insurance number, marital status, gender, preferred language, seniority service date, birth date, department, group code, and union code. The corporation also informs the investment firm when it awards cash bonuses, but does not specify the recipient or the amount of the bonus. The RRSP and savings plan was established by the corporation in fulfillment of a commitment under its collective agreement with the employees' union. The corporation pays the investment firm for the services it provides under the plan and does not disclose the information to the investment firm for consideration, monetary or otherwise.

Commissioner's Findings (Issued October 18, 2001)

Jurisdiction: As of January 1, 2001, the *Personal Information Protection and Electronic Documents Act* applies strictly to federal works, undertakings, or businesses or to disclosures of personal information across borders for consideration. The corporation in question is neither a federal work, undertaking, or business as defined in the *Act*, nor does it disclose the personal information at issue across borders for consideration.

The Commissioner concluded that he lacked jurisdiction to pursue the matter further.

Requester alleges non-receipt of credit report from agency [Section 8]

Complaint

An individual complained that a credit-reporting agency refused his request to disclose his credit report to him.

Summary of Investigation

The complainant had written to the credit reporting agency to request access to any credit report the agency held on him. In his complaint, he alleged that he did not subsequently receive a response from the agency. The agency's consumer relations centre has a staff of six who are responsible for receiving and processing access requests according to standard procedures. By those procedures, a client request is not filed unless it has been matched to a credit report that has either been mailed or handed to the client. The centre does have on file a copy of the complainant's access request, with a handwritten notation to the effect that a response was mailed to the complainant's correct address 13 days after receipt of the request. The mailing of a response was also confirmed by reference to a computerized log and a computer-generated audit report. The complainant at one point allowed the possibility of having merely overlooked the credit report on receiving it. Later he declared it highly unlikely that he had received the report without noticing it.

Commissioner's Findings (Issued October 26, 2001)

Jurisdiction: As of January 1, 2001, the *Personal Information Protection and Electronic Documents Act* applies to disclosures of personal information across borders for consideration. The Commissioner had jurisdiction in this case because the credit reporting agency in question had disclosed personal information across borders for consideration.

Application: section 8(3) of the *Act* states that an organization shall respond to a request with due diligence and in any case not later than 30 days after receipt of the request. Section 8(5) states that if the organization fails to respond within the time limit, the organization is deemed to have refused the request.

The Commissioner found no reason to doubt the evidence that the credit-reporting agency had received the complainant's access request and mailed a response within the time limit prescribed. He found that the agency had complied with section 8(3) of the *Act*.

The Commissioner concluded that the complaint under section 8(5) was not well-founded.

Airline accused of refusing access to personal information about vacation incidents [Principles 4.1 and 4.9, Schedule1]

Complaint

Three air travellers complained that an airline company had denied them access to personal information about their experiences during a Mexican vacation.

Summary of Investigation

The complainants had requested access to all personal information the airline and its travel affiliate held regarding certain incidents they had experienced during a vacation in Mexico. A representative responded initially that the company was under no obligation to provide such information. On being advised of its obligations under the *Personal Information Protection and Electronic Documents Act* by the Office of the Privacy Commissioner, the company took immediate action to appoint an official to be accountable for compliance with the *Act*, processed the complainants' access request, and sent them the personal information requested. On reviewing this information, the complainants were of the opinion that the company had not included incident reports. The investigator for the Privacy Commissioner examined the company's original files containing the complainants' personal information, but found no evidence of information other than that which the complainants had already received. The company confirmed in writing that it did not have in its possession any additional information about the complainants, including incident reports.

Commissioner's Findings (Issued October 31, 2001)

Jurisdiction: As of January 1, 2001, the *PIPED Act* applies to federal works, undertakings, or businesses. The Commissioner had jurisdiction in this case because airlines are federal works, undertakings, or businesses, as defined in the *Act*.

Application: Principle 4.1, Schedule 1, states that an organization is responsible for personal information under its control and shall designate an individual or individuals who are accountable for the organization's compliance with [the principles in] Schedule 1. Principle 4.9 states that upon request, an individual shall be informed of the existence, use, and disclosure of his or her personal information and shall be given access to that information.

Regarding Principle 4.1, the Commissioner determined that the airline company had not designated an individual until his Office intervened. He found therefore that the company had initially failed to comply with this principle. However, he also noted that the company had subsequently designated a senior official responsible for ensuring compliance with the *Act*. The Commissioner considered this issue resolved.

Regarding Principle 4.9, the Commissioner likewise determined that the company had provided the complainants with their personal information only after intervention by his Office. He found therefore that the company had not initially been in compliance with this principle. He noted, however, that the complainants were satisfied that they had received all of their personal information in the company's possession; they were also satisfied with the outcome of the investigation.

The Commissioner concluded that the complaint was well-founded and resolved.

Employee objects to employer's use of bank account number on pay statement [Principles 4.3 and 4.7, Schedule 1]

Complaint

An employee of a telecommunications company complained that her employer:

1. Used her personal information for a purpose without her consent by printing her bank account and bank transit numbers on her pay statements; and
2. Did not adequately safeguard employees' pay statements given the sensitivity of the information in them.

Summary of Investigation

The employees of the telecommunications company in question receive their pay by direct deposit and their pay statements by delivery in sealed envelopes at the workplace. As a result of a merger and a subsequent conversion of payroll systems, bank account and bank transit numbers began to be included on all employees' pay statements as of January 1, 2001. Printing of such numbers on pay statements has become standard practice in both the private and the public sectors. On this company's statements, there is no indication what the numbers refer to; only a person familiar with the bank's information codes would know what the numbers represent. On delivery to the complainant's workplace, the sealed envelopes containing employees' pay statements are collected together in a larger envelope and left on a manager's desk, where they often remain unsecured and largely unattended for periods as long as 24 hours.

The complainant had originally consented to having her pay deposited directly into her bank account, but had never explicitly consented to having the numbers appear on her statement. She believed that her employer was thus using her personal bank account information without her consent and for a purpose inconsistent with that for which she originally had provided it. She also believed that her employer did not adequately safeguard employee pay statements at her workplace.

The company's position was that the information was still being used only for the original purpose of directly depositing payroll funds; that the practice of printing account and

branch numbers on pay statements had become imperative for purposes of verifying allocations of funds and resolving discrepancies; and that many employees had already come to expect and rely upon the appearance of these numbers on their statements. The company also argued that it did adequately safeguard its employees' bank account information by delivering statements in confidential sealed envelopes.

Commissioner's Findings (Issued November 5, 2001)

Jurisdiction: As of January 1, 2001, the *Personal Information Protection and Electronic Documents Act* applies to federal works, undertakings, or businesses. The Commissioner had jurisdiction in this case because telecommunications companies are federal works, undertakings, or businesses as defined in the *Act*.

Application: Principle 4.3, Schedule 1, states that the knowledge and consent of the individual are required for the collection, use, or disclosure of personal information, except where inappropriate. This principle also stipulates (4.3.5) that the reasonable expectations of the individual are relevant. Principle 4.7 states that personal information shall be protected by appropriate security safeguards appropriate to the sensitivity of the information.

On the first aspect of the complaint (consent), the Commissioner determined that employees who provide their bank account and bank transit numbers for direct-deposit purposes could reasonably expect those numbers to appear on transaction records for the entirely consistent purpose of verifying proper allocation of funds. He was satisfied that the complainant had thus implicitly given consent. He found that the company therefore had met its obligations under Principle 4.3, Schedule 1.

The Commissioner concluded that this aspect of the complaint was not well-founded.

On the second aspect of the complaint (security safeguards), the Commissioner determined that the company's operational controls at the complainant's workplace were not consistent with the sensitivity of the personal information contained in the pay statements. He found that the company did fail to meet its obligations under Principle 4.7, Schedule 1.

However, he noted that the company, on being informed of its obligations, had taken immediate and appropriate steps to correct its information management practices related to employee pay statements.

The Commissioner concluded that this aspect of the complaint was well-founded and resolved.

Further Considerations

As a short-term solution, the company agreed to implement tighter operational controls at the complainant's own workplace and offered the complainant the option of having her pay statement mailed to her home.

Company asks for customer's SIN as matter of policy [Principles 4.3.3 and 4.4.1, Schedule 1; and section 5(3)]

Complaint

An individual complained that a telecommunications company had improperly collected her personal information in the form of her Social Insurance Number (SIN).

Summary of Investigation

In signing-up the complainant for Internet connection, the telecommunications company in question had asked her for her SIN. According to the complainant, the company representative with whom she had spoken had told her, "No SIN, no connection," and she had therefore felt obliged to give up her number in order to obtain the service. It was the company's written policy to collect SINs from persons requesting services. The purpose of this policy was to avoid confusion over similar names among customers. However, by the same policy, the company did not insist on obtaining the SIN in cases where the customer refused and did advise its employees that the collection was not obligatory.

Commissioner's Findings (Issued November 5, 2001)

Jurisdiction: As of January 1, 2001, the *Personal Information Protection and Electronic Documents Act* applies to federal works, undertakings, or businesses. The Commissioner had jurisdiction in this case because telecommunications companies are federal works, undertakings, or businesses, as defined in the *Act*.

Application: Principle 4.3.3, Schedule 1, states that an organization shall not, as a condition of the supply of a product or service, require an individual to consent to the collection, use, or disclosure of information beyond that required to fulfil the explicitly specified and legitimate purposes. Principle 4.4.1 states that organizations shall not collect personal information indiscriminately. Both the amount and the type of information collected shall be limited to that which is necessary to fulfil the purposes identified. Section 5(3) states that an organization may collect, use, or disclose personal information only for purposes that a reasonable person would consider are appropriate in the circumstances.

Regarding Principle 4.4.1, the Commissioner determined that, by the company's own policy, the collection of SINs was non-obligatory and therefore not necessary to fulfil explicitly specified and legitimate purposes. He found that the collection was thus indiscriminate and that the company was not in compliance with this principle.

Regarding Principle 4.3.3, the Commissioner was satisfied that the complainant had clearly received the impression that giving her SIN was a condition of service. He found therefore that the company was not in compliance with this principle.

Regarding section 5(3), the Commissioner was mindful of his Office's longstanding position that the SIN should not be used as a universal identifier and that citizens should not give out their SINs unless legally required to do so for purposes of the limited number of federal government programs authorized for such collection. He was satisfied that a reasonable person would object to the collection of SINs for purposes of Internet connection. He found that the company was therefore not in compliance with section 5(3).

The Commissioner noted that the company had removed the SIN from the complainant's file and was in the process of changing its policy so that SINs would no longer be requested.

The Commissioner concluded therefore that the complaint was well-founded and resolved.

Further Considerations

The Commissioner also recommended that the company take steps to review its files and remove any other unnecessary SINs collected from its other customers.

User accuses ISP owner of reading and blocking her e-mail [Principle 4.3, Schedule 1]

Complaint

An individual complained that the owner of her former Internet service provider (ISP):

1. Had improperly collected her personal information without her consent in that he had read her e-mails; and
2. Was blocking e-mail she was attempting to send through a new ISP to users of her former ISP.

Summary of Investigation

The complainant had been a subscriber with a certain ISP for two years. During that time, she had had a disagreement with the ISP owner concerning her use of her account, specifically her attempts to transmit large files by e-mail. She alleged that during that disagreement the owner had told her that he could read her e-mails. She further alleged that, after she had moved to another city and subscribed with a different ISP, the same owner had begun to block the e-mails she was trying to send to users of her former ISP.

The owner in question said that he could not remember any disagreement with the complainant, but he did allow that, on detecting a large number of "delivery failure" messages (indicating attempts to transmit large files by e-mail), it would have been his usual practice to call the user and discuss the matter. He denied being able to read anything other than "delivery failure" messages in relation to the complainant's account. He also denied blocking her messages.

The investigation confirmed that the ISP in question can monitor users' account activity and detect "delivery failure" messages, but does not receive e-mails or attachments and cannot read the content of users' e-mail messages. Nor was there any evidence that the owner had been blocking the complainant's

e-mails from her new server. In fact, several weeks before the owner was notified of the complaint against him, the blocking problem ceased when a computer technician changed the Internet protocol address on the complainant's computer.

Commissioner's Findings (Issued November 5, 2001)

Jurisdiction: As of January 1, 2001, the *Personal Information Protection and Electronic Documents Act* applies to federal works, undertakings, or businesses. The Commissioner had jurisdiction in this case because Internet service providers are federal works, undertakings, or businesses as defined in the *Act*.

Application: Principle 4.3, Schedule 1, states that the knowledge and consent of the individual are required for the collection, use, or disclosure of personal information, except where inappropriate.

The Commissioner was satisfied that the ISP could not read its users' e-mails and had not blocked the complainant's messages. He also determined that a reasonable person would expect the ISP to monitor the services it provides and respond to persistent "delivery failure" messages. He found that the ISP in this case was not in contravention of Principle 4.3, Schedule 1.

The Commissioner concluded therefore that the complaint was not well-founded.

Employer sends third parties copies of response to employee's access requests [Principles 4.3 and 4.5, Schedule 1; and section 5(3)]

Complaint

An employee of an airport authority complained that her employer had, without her consent, disclosed to three third parties her personal information in the form of copies of a letter of response to access requests she had made.

Summary of Investigation

The complainant had submitted requests under the *Personal Information Protection and Electronic Documents Act* for access to information held by her employer. The employer subsequently sent her a letter of response to the effect that the organization was refusing her requests. This letter also indicated that copies were being sent to three other persons – specifically, two union representatives and the coordinator of employee relations at the airport. The complainant had not sent copies of her access requests to these parties and had not explicitly consented to having copies of the response letter sent to them.

The union representatives had previously attended the meeting at which the issue of access to the complainant's personal information had first been raised. The employee relations coordinator had previously intervened in a harassment complaint filed by the same complainant and had in his possession certain

related documents to which the complainant had requested access. On the grounds of these prior involvements, the employer argued that the complainant had implicitly consented to the disclosures. The complainant maintained that she had submitted the access requests personally on her own behalf, without union intervention.

Commissioner's Findings (Issued November 5, 2001)

Jurisdiction: As of January 1, 2001, the *Personal Information Protection and Electronic Documents Act* applies to federal works, undertakings, or businesses. The Commissioner had jurisdiction in this case because airports are federal works, undertakings, or businesses, as defined in the *Act*.

Application: Principle 4.3, Schedule 1, states that the knowledge and consent of the individual are required for the collection, use, or disclosure of personal information, except where inappropriate. Principle 4.5 states that personal information shall not be used or disclosed for purposes other than those for which it was collected, except with the consent of the individual or as required by law. Section 5(3) states that an organization may collect, use, or disclose personal information only for purposes that a reasonable person would consider appropriate in the circumstances.

Regarding Principle 4.3 and the disclosure to the union representatives, the Commissioner determined that there would have been implied consent for the employer to send response copies to those parties only if the complainant had indicated that she had sent them copies of her access requests. The complainant had the right to exercise her formal recourse without union intervention, and it was not necessary for the employer to inform the union of its response. The Commissioner found that no implied consent had existed as far as the union representatives were concerned. Furthermore, in consideration of section 5(3), he was satisfied that a reasonable person would have considered the disclosure to the union representatives to be unacceptable.

He concluded therefore that this aspect of the complaint was well-founded.

Regarding Principle 4.5 and the employee relations coordinator, given the direct involvement of that party in the access request, the Commissioner determined that it had been appropriate for the employer to inform him of its decision to refuse the complainant access to the documents she had requested. Furthermore, in consideration of section 5(3), the Commissioner was satisfied that a reasonable person would have considered the communication to the employee relations coordinator to be acceptable. He found that the employer was thus in compliance with Principle 4.5 as far as the employee relations coordinator was concerned.

He concluded therefore that this aspect of the complaint was not well-founded.

Further Considerations

During the investigation, the Office of the Privacy Commissioner advised the airport authority in question that it is preferable not to send copies of responses to third parties, but rather to allow the individual requester to judge whether or not to share a response with others after receiving it. The Commissioner was pleased to note that the organization had followed this advice in dealing with subsequent access requests by the complainant.

Telephone company demands identification from new subscribers [Principles 4.2, 4.2.3 and 4.3, 4.3.2, 4.3.3 Schedule1; and section 5(3)]

Complaint

An individual complained that a telecommunications company's collection of personal information from new subscribers was inappropriate, in that the company required a deposit from new customers who refused to supply the information.

Summary of Investigation

When the complainant attempted to obtain a new telephone service from the company in question, an operator asked her to supply two pieces of personal identification. When the complainant expressed reluctance, the operator told her that she would have to provide a deposit if she did not comply. The operator also told her that the purpose of the information collection was to confirm her identity. A company supervisor subsequently gave her the same explanation for the collection and confirmed that she would have to provide a deposit if she did not supply the information.

It is company policy for operators to ask new subscribers for two pieces of identification, to demand a deposit in cases of refusal, and to explain the information collection simply as confirmation of identity. However, in cases where an applicant is a new customer with no previous business relationship with the company, the actual purpose of the collection is to run a credit check on the applicant, in accordance with CRTC regulations, given that the provision of telephone services constitutes an extension of credit on the company's part.

Commissioner's Findings (Issued November 8, 2001)

Jurisdiction: As of January 1, 2001, the *Personal Information Protection and Electronic Documents Act* applies to federal works, undertakings, or businesses. The Commissioner had jurisdiction in this case because telecommunications companies are federal works, undertakings, or businesses, as defined in the *Act*.

Application: Principle 4.2.3 states that purposes should be identified at or before the time of collection. Principle 4.3.2 states that organizations must make a reasonable effort to advise the individual concerned of the purposes for which the information will be used and must do so in such manner that the individual can reasonably understand.

Principle 4.3.3 states that organizations must not, as a condition of supplying a product or service, require an individual to consent to the collection, use, or disclosure of information beyond that required to fulfil the explicitly specified and legitimate purposes. Section 5(3) states that an organization may collect, use, or disclose personal information only for purposes that a reasonable person would consider appropriate in the circumstances.

Regarding Principle 4.3.3 and section 5(3), the Commissioner determined that a reasonable person would consider it appropriate for the company to collect personal information for the purpose of confirming whether a potential customer is credit worthy or, in the case of repeat customers, confirming identity.

He concluded that this aspect of the complaint was not well-founded.

Regarding Principles 4.2.3 and 4.3.2, the Commissioner determined that a reasonable person would conclude that the company did not explicitly state the purpose for its collection of personal information with respect to first-time subscribers.

He concluded that this aspect of the complaint was well-founded.

Further Considerations

The company agreed to amend its practice in identifying purposes. Specifically, the company will inform first-time subscribers that the purpose of its information collection is to assess credit-worthiness given that the company supplies credit in the form of long-distance calling service.

Broadcaster accused of collecting personal information via Web site [Section 2; and Principle 4.3, Schedule 1]

Complaint

An individual complained that a broadcaster had attempted, through its advertising server, to collect his personal information, specifically the NETBIOS information on his computer, without his consent.

Summary of Investigation

The complainant had a computer equipped with both a cable modem for Internet connection and a firewall designed to detect and block attempts at intrusion. Every time he tried to log onto the organization's Web site, his firewall detected, rejected, and reported on, an attempt by the broadcaster's advertising server to gain access to the NETBIOS information on his computer. A NETBIOS is a computer's common or "friendly" name related to its Internet protocol (IP) address. If an IP address is traced, it allows access to information such as Web sites visited by the computer's user or recent passwords used in obtaining access to secure accounts. The likelihood of tracing an IP address is small if the user has dial-up Internet access, but significantly greater if the user has a fixed Internet connection via a cable modem, as was the case with the complainant.

After conducting internal inquiries, the organization confirmed that the complainant's allegation was true. The broadcaster explained that the network administrator, on installing Microsoft Windows NT, had neglected to deactivate certain features that come automatically with that program. These features, known as Internet Name Services, enable a server to collect the NETBIOS information of Web site users. Once informed that the features were on, the network administrator promptly turned them off. The complainant subsequently confirmed that his firewall no longer detected any attempts by the organization to obtain his NETBIOS information.

Commissioner's Findings (Issued November 20, 2001)

JURISDICTION: As of January 1, 2001, the *Personal Information Protection and Electronic Documents Act* applies to federal works, undertakings or businesses. The Commissioner had jurisdiction in this case because broadcasters are federal works, undertakings or businesses, as defined in the *Act.*

APPLICATION: section 2 of the *Act* defines personal information to be "… information about an identifiable individual …". Principle 4.3 of Schedule 1 states that the knowledge and consent of the individual are required for the collection, use, or disclosure of personal information, except where inappropriate.

The Commissioner was satisfied that in some circumstances, notably the complainant's, a NETBIOS might be used to obtain information traceable to an identifiable individual. He determined therefore that the information at issue was personal information for purposes of the *Act*.

The Commissioner found that the broadcaster had failed to meet its obligations under Principle 4.3. However, he did not dispute the broadcaster's explanation that this failure had been unintentional, and he noted that its response had been satisfactory.

He concluded therefore that the complaint was well-founded and resolved.

Couple alleges bank withheld loan information [Sections 8(3) and 8(5)]

Two Complaints

A husband and wife complained in two separate complaints that a bank had denied them access to their personal information in that it had not responded to their request for information related to a loan application.

Summary of Investigation

The complainants had written, jointly signed, and submitted two letters requesting personal information about two different credit products from their local branch of the bank in question. The letters were identical, except for their subject lines, one of which referred to a numbered loan application and the other to a

numbered mortgage, both relating to the complainants. Within the month, the bank sent them the information they had requested about their mortgage, but no information about their loan application. The complainants wrote the bank another letter, outlining in greater detail the information they were seeking about the loan application. Approximately one month after this second submission, a lawyer for the bank responded, informing the complainants only that they would be required to pay photocopying charges of 25 cents per page. The complainants then submitted another letter in which they enclosed a cheque to cover reproduction costs and confirmed that they still wanted the information in question. When they received no further response after three weeks, they filed their complaints with the Office of the Privacy Commissioner.

The bank at first denied the allegation, insisting that the complainants' second submission had been the first to make reference to the loan application. However, on being presented with a copy of the letter containing the prior reference, the bank checked its records and acknowledged receipt of that earlier letter. The bank explained that its failure to respond had been unintentional, in that the employee who had received the first submission had not noticed the different subject headings on the two similar-looking letters, had assumed they were identical, and had therefore forwarded only one of them (the one referring to the mortgage) on for response.

Commissioner's Findings (Issued November 26, 2001)

Jurisdiction: As of January 1, 2001, the *Personal Information Protection and Electronic Documents Act* applies to federal works, undertakings, or businesses. The Commissioner had jurisdiction in this case because banks are federal works, undertakings, or businesses, as defined in the *Act*.

Application: Section 8(3) of the *Act* states that an organization shall respond to a request with due diligence and in any case not later than thirty days after receipt of the request. Section 8(5) states that if the organization fails to respond within the time limit, the organization is deemed to have refused the request.

The Commissioner found that the bank had failed to respond within the time limit and was thus in contravention of section 8. However, he was satisfied that this failure had been unintentional, and he noted that the bank had subsequently provided to the complainants all the information they had sought.

He concluded therefore that the complaints were well-founded and resolved.

Incidents under *PIPED Act*

Incidents are matters that come to my attention through various sources including issues raised in the media. These are usually issues where there is no identified victim and where no complaint has been filed. During the past 11 months my Office has looked into the following two incidents.

Transportation company collects, discloses passengers' personal information

Incident

It was alleged that a transportation company's sales agents were:

1. asking for date of birth and citizenship as well as name from individuals making train bookings by phone or in person for the Toronto-to-New York run; and
2. disclosing this information to United States Customs (USC) and the United States Naturalization and Immigration Service (USNIS).

Summary of Investigation

The Canadian company confirmed that the practice in question has been taking place since December 2000, by agreement among the company, the U.S. transportation company, Canada Customs and Revenue Agency, and USC/USNIS. The purpose is to minimize delays at the Canada/U.S. border. The personal information thus collected is stored in the company's reservation computer system and deleted if the individual does not eventually purchase the ticket. If the passenger does purchase the ticket, his or her name, date of birth, and citizenship are printed on a manifest, which is then faxed to USC/USNIS and a copy given to the service manager on board the train. The service manager destroys the manifest shortly after the trip is completed.

The Office of the Privacy Commissioner of Canada determined that the sales agents, on written instruction from the company, had been representing the practice as a requirement for passengers on the Toronto-to-New York run.

Outcome

The company asked the Office of the Privacy Commissioner of Canada for instructions on an acceptable resolution to the problem. The Office advised that it issue to its sales agents a clear directive to the effect that passengers' provision of date of birth and citizenship must be represented as voluntary and that agents may, after booking a ticket, ask customers whether they would be willing to provide this information in order to facilitate customs clearance at the border.

On receiving a copy of such a directive sent by the company to its sales agents, the Office informed the company that the incident file would be closed, subject to the Office's continued monitoring of sales agents' booking practices. The Office also advised that at some point the company send its sales agents a follow-up note clarifying in stronger terms that they are not to collect personal information at the time of booking without the informed consent of the individual.

Web site broadcasts cell phone conversations

Incident

The *Ottawa Sun* reported on June 7, 2001, that an Ottawa-based Web site was streaming live audio from cellular telephones onto the Internet from a radio.

A scanner was intercepting cellular telephone traffic. The scanner was connected to a computer that was hosting a Web site. By connecting to the Web site, anyone could listen in on private cell phone conversations.

Outcome

As the Office of the Privacy Commissioner began its investigation, the Internet service provider (ISP) in question shut down the Web site because of bandwidth problems. This was caused by an employee who had a personal network account that had been forwarding data through another server. On discovery, the ISP had immediately relieved the employee of his duties. The ISP indicated that the Web site in question had moved to a New York server under new management.

Given that the Ottawa-based Web site had been shut down, the Office's investigation was discontinued. The Web site will be monitored periodically for an indefinite length of time.

Inquiries by type under *PIPED Act*

January 1, 2001 to November 30, 2001

Subject	Number
Criminal records	30
Drug Testing	3
Encryption	7
Financial Institutions	1,519
Identity Theft	38
Information Request	2,558
Interception/monitoring	154
Interpretation	2,024
Jurisdiction	1,975
Marketing	439
Medical Records	137
Calls from Members of Parliament	7
Publication Requests	675
Social Insurance Number	1,834
Telecommunications	786
Transportation	139
Other	388
Total	12,713

Privacy Practices and Reviews

The *Personal Information Protection and Electronic Documents 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*.

Following accepted standard audit objectives and criteria, the Privacy Practices and Reviews Branch of my Office will conduct compliance reviews and audits under section 18 of the *Act*. As it has come into effect at the beginning of this year, I have not yet initiated any such audit. I have focused instead on educating businesses and organizations on the impact of the new legislation, and giving them guidance for establishing privacy policies that comply with it.

In the Courts

Mathew Englander v. Telus Communications Inc.

This is the first application for judicial review to be filed in the Federal Court under the *PIPED Act*. Mathew Englander filed a complaint with the Office of the Privacy Commissioner on January 1, 2001 claiming, *inter alia,* that Telus uses and discloses customers' names, addresses and telephone numbers in its White Pages directories and otherwise, without customers' knowledge and consent and that Telus inappropriately charges customers for choosing to have their telephone number "non-published". The applicant submitted that these actions by Telus contravene subsections 5(1) and (3) of the *PIPED Act* as well as several clauses of Schedule 1 of the *PIPED Act.*

After investigating the complaint, I concluded that Telus is in full compliance with the *Act* in respect of the matters of which the complaint was made. I concluded that a reasonable person would consider Telus' initiation of service practice and subsequent publishing of customers' personal information in its white pages is an appropriate collection, use and disclosure of the information. I further concluded that Telus has the authority to charge its customers a fee for non-published telephone

service and that this is not an unreasonable practice so as to contravene principle 4.3.3 of Schedule 1.

I found the complaint not well-founded. As permitted by section 14 of the *PIPED Act,* Mr. Englander has applied to the court for a hearing in respect of the matter.

Ronald G. Maheu v. The Attorney General of Canada and IMS Health Canada

The applicant has applied for a hearing in the Federal Court, as permitted under section 14 of the *PIPED Act,* after having complained to me that IMS Health improperly discloses personal information by gathering and selling data on physicians' prescribing patterns without their consent.

After having investigated the matter, I found that prescription information, whether in the form of an individual prescription or in the form of patterns discerned from many prescriptions, is not personal information about a physician. In determining whether the information at issue was personal information within the meaning, scope and purpose of the *Act*, I took the view that the meaning of "personal information", though broad, is not so broad as to encompass all information associated with an individual. I found that an individual prescription, though potentially revealing about a patient, is not in any meaningful sense about the prescribing physician as an individual but is about the professional process that led to its issuance and should be regarded as a work product – that is, the tangible result of the physician's work activity. In sum, I concluded that the complaint was not well-founded.

Mr. Maheu has applied to the court for a hearing in respect of this matter. Included in the Notice of Application was a request by the applicant, under the Federal Court rules, that my Office transmit material in its possession to the applicant and the Registry of the Federal Court. The Office of the Privacy Commissioner has objected to the request, as all documents not already in the possession of the applicant cannot be disclosed by the Privacy Commissioner pursuant to provisions of the *PIPED Act.*

Communications and Public education

Under the *PIPED Act,* my Office was given a broader mandate for public education in order to increase awareness and understanding of privacy issues. To focus on this important new responsibility, establishing the Communications and Strategic Analysis Branch was one of the first steps I took following my appointment. This branch has undertaken a number of activities during the past year to help raise awareness of privacy issues and to inform Canadian citizens and businesses about the new private sector legislation.

Public speaking is an invaluable tool that helps me fulfill my responsibility for promotion, public education and awareness of privacy issues. I have given 35 speeches to a range of organizations across Canada and internationally over the past year. Another 31 speeches were delivered by other senior staff. Speeches have focused on the major issues of the day, such as the security versus privacy debate that ensued following the Sept. 11 attacks on the U.S. Many other speaking engagements have been used to tell citizens and businesses alike about the new *Act* and how it affects them, to discuss privacy in the workplace, and to raise privacy concerns about specific initiatives, including Government On-Line, electronic health records and the growing use of video surveillance.

As well, recognizing the influence of the media in setting the agenda for public debate and in raising public awareness, my Office has begun to proactively track privacy issues in the media and has become much more engaged in a variety of media relations activities.

These activities have included disseminating public statements, news releases and feature articles to both mainstream and targeted media; granting media interviews and participating in editorial board meetings; and providing media relations support for speeches, conferences and other special events. In addition, my Office has responded to inquiries from the media, providing comment and background information on a wide variety of privacy-related issues.

Every month, the number of media queries continues to increase, currently averaging anywhere from 80 to 100 per month. In addition, I have granted more than 210 media interviews since September 2000.

Public education materials

My Office has produced and distributed promotional and educational material to satisfy an increased demand for information under the *PIPED Act.* We have published comprehensive guides to the new *Act* for both businesses and individuals. More than 21,000 of both of these guides have been distributed during 2001.

In addition, we have created posters, privacy kits, notepads and bookmarks. All these products help to satisfy the demand for more information on privacy issues by individuals, businesses and other organizations.

Advertising

As part of the public outreach program to raise awareness of the new privacy rights of Canadians in the private sector, beginning with federally regulated businesses, my Office placed advertisements in more than 1,300 daily and community newspapers in all parts of Canada, These ads were directed at informing Canadians of their rights under the *PIPED Act.* The advertisement, under the banner "Your privacy is our concern" and « Votre vie priveé, ça nous regarde », which ran in March 2001, reached millions of Canadians in all regions of the country.

A second advertisement ran in the 12 newspapers in the three territories, pointing out that the *Personal Information Protection and Electronic Documents Act* applies to all businesses in the territories as they are considered to be federal works and undertakings. Following the appearance of the advertisements, my Office noted a significant increase in the number of inquiries and requests for further information about the *PIPED Act.*

Web Site

Over the past year, my Office's Web site has undergone a complete redesign and considerable expansion as part of our greater mandate for public education and awareness under the new *Act*.

Every effort is made to ensure the Web site is an up-to-date resource for privacy information, as well as a useful tool for research on privacy-related issues. Ultimately, the redesigned Web site is more interactive, user-friendly and relevant to both individuals and businesses.

I am pleased to report that the Web site is an increasingly efficient tool for reaching Canadians and others with information about privacy issues. Visits to our site continue to increase, with an average of 11,500 visits per month.

Communications Activities

January 1, 2001 to November 30, 2001

Activity		Number
Speeches delivered by Privacy Commissioner		35
Speeches delivered by senior staff		31
News Releases		15
Media Interviews		210
Distribution of materials		**27,586**
Business Guides	13,005	
Citizen's Guides	8,707	
Other (Annual Reports, bookmarks, fact sheets, *Act*s, etc.)	5,874	
Average number of visits to Web site per month		11,500

Part Three
Corporate Services

Gearing up for implementation of the Private Sector Act

The Office has increased the size of its staff and budget to prepare for implementation of the *Personal Information Protection and Electronic Documents Act,* which started coming into effect January 1, 2001.

Our budget was increased to more than $11 million per year beginning April 1, 2001, up from $8.7 million for 2000-2001. This budget increase enabled my Office to make a number of important changes, which included:

- increasing inquiries staff to handle an increase in the number of calls;
- extending our hours from 9 a.m. to 5 p.m. in all time zones across Canada;
- establishing the Privacy Practices and Reviews Branch to handle audits under the *Personal Information Protection and Electronic Documents Act* and to continue work in the public sector;
- establishing a Communications and Strategic Analysis Branch, incorporating the existing research function, to focus on communications and public education, and to ensure that we are a centre of expertise on issues related to privacy; and
- increasing the number of investigators to handle complaints under both *Acts*.

A long-term financial framework for future funding will be presented to the Treasury Board of Canada Secretariat in 2003-2004.

Resources

(April 1, 2000 to March 31, 2001)

	FTEs	Expenditure Totals	Percentage of Total
Privacy	56	$ 7,418,451	89%
Corporate Services	10	$ 941,369	11%
Total	**66**	**$ 8,359,820**	**100%**

Note: FTE stands for "full-time equivalent" or full-time staff.

Detailed Expenditures[1]

April 1, 2000 to March 31, 2001

	Privacy	Corporate Services[2]	Total
Salaries	$3,776,280	$464,091	$4,240,371
Employee Benefit Plan Contributions	611,000	84,500	695,500
Transportation and Communication	268,588	93,470	362,058
Information	979,136	1,993	981,129
Professional Services	600,427	121,197	721,624
Rentals	33,036	13,958	46,994
Repairs and Maintenance	327,711	32,721	360,432
Materials and Supplies	62,616	28,400	91,016
Acquisition of Machinery and Equipment	759,403	100,998	860,401
Other Subsidies and Payments	254	41	295
Total	**$7,418,451**	**$941,369**	**$8,359,820**

Notes:

[1] Expenditure figures do not incorporate final year-end adjustments.

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

Corporate Structure