Annual Report
Privacy Commissioner
1998-99

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

(613) 995-2410, 1-800-267-0441
Fax (613) 947-6850
TDD (613) 992-9190

Cat. No. IP 30-1/1999
ISBN 0-662-64334-8

This publication is available on audio cassette, computer diskette and on the Office's Internet home page at http://www.privcom.gc.ca

Privacy Commissioner of Canada

Commissaire à la protection de la vie privée du Canada

July 1999

The Honourable Gildas L. Molgat
The Speaker
The Senate
Ottawa

Dear Mr. Molgat:

I have the honour to submit to Parliament my annual report which covers the period from April 1, 1998 to March 31, 1999.

Yours sincerely,

Bruce Phillips

Bruce Phillips
Privacy Commissioner

Privacy Commissioner of Canada

Commissaire à la protection de la vie privée du Canada

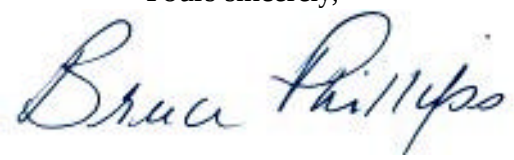
July 1999

The Honourable Gilbert Parent
The Speaker
The House of Commons
Ottawa

Dear Mr. Parent:

I have the honour to submit to Parliament my annual report which covers the period from April 1, 1998 to March 31, 1999.

Yours sincerely,



Bruce Phillips
Privacy Commissioner

Our thanks to Chris Slane, a professional cartoonist and son of New Zealand Privacy Commissioner Bruce Slane, for permission to reproduce the cartoons from his latest collection *Let me through, I have a morbid curiosity.*

Did You Know…?

Not worried about your privacy? Perhaps you should think again. Here are just a few of the stories we heard in the past year.

- A.C. Neilson, the market rating company, has patented a facial recognition system which secretly identifies shoppers to track their buying habits.
- Two Ontario grocery stores asked welfare recipients to thumbprint their cheques before cashing them. Ontario welfare cards contain digitized thumbprints. Both stores stopped after a shopper complained to the Ontario Privacy Commissioner.
- Police caught a Toronto-area group secretly videotaping debit card users entering their PINs, tapping stores' phone lines to steal the data, then using it to empty customers' accounts.
- What you eat, wear, watch, ride in and play with is increasingly tracked by companies to uncover patterns of consumer behavior—for example, marketers discovered that men who go out to buy diapers in the evening are more likely to pick up beer on the way home.
- Some Web sites track "click stream" data—what pages you view and what information you download, and some leave "cookies"—data that helps the site identify you next time you visit.
- Employers now can check out job applicants' Web surfing to examine their hobbies, interests and attitudes. According to a Calgary security-management corporation doing background checks, "a (Web) search can tell a lot about a person, good and bad."
- The Québec government is considering creating a central computer database on every Québecer, including names, photographs, and basic identifying information.
- Nissan Web site visitors who wanted information its new Xterra sport utility vehicle got a whole lot more—the e-mail addresses of 24,000 other potential buyers.
- Several chain stores admit giving law enforcement agencies the shopping habits of their loyal customer card holders.

- Urine samples cannot tell whether someone is "high" on drugs, only whether he or she has used the drug in the past 30 days.
- Your employer can read your e-mail, access your computer files, track your Internet traffic and listen to your voice mail.
- If you're one of 7.2 million Air Miles Cardholders, every time you swipe that card you're sharing your buying decisions with 134 corporate sponsors. The company sorts and packages the data on behalf of its corporate sponsors and "anything Blockbuster Video knows about an individual's viewing preferences, the local liquor outlet can know too—and vice versa".
- Some of that personal information—Air Miles card number, name, home phone numbers, e-mail addresses, business name and phone number—on hundreds of Air Miles cardholders was put on the Web for several months and possibly for as long as a year.
- The Michigan Commission on Genetic Privacy is reportedly proposing that the state permanently store blood samples of newborns it obtained to detect rare congenital diseases because the samples are a valuable resource for law enforcement authorities and scientific research.
- Removing names from personal information and combining it with other peoples' data does not necessarily protect it. "Reverse engineering" allows researchers to identify individuals in aggregate statistical information by combining it with public information. For example, if you know five per cent of people in a block of 20 people are over 65 and earn more than $100,000, you can find 67-year old Jane Doe in public records and infer her income.
- Several British companies are consulting scientists on implanting microchips in employees to monitor their whereabouts and timekeeping. One scientist has developed and had a chip implanted to demonstrate how well it works.
- Internet service provider America Online receives a steady stream of court orders for information about subscribers, during divorce and child custody cases.

Table of contents

The Age of Surrender?

We begin with neither bang nor whimper, but with some questions:

Is privacy worth saving?

Is the beginning of a new millennium to signal the ending of the right to a private life?

Is the age now upon us to be the Age of Surrender?

These questions are neither merely rhetorical nor theoretical. They are being asked in more and more places. As we went to press, we noted a spate of mainstream publications taking up this issue. Their despairing conclusions could be summed up this way: Technology has won. Human rights have lost. Privacy is Dead. Get used to it.

The most trenchant summary of this viewpoint appeared May 1 in the highly-respected periodical *The Economist*. Observing that society has already reached a state of pervasive surveillance (a point made here many times), *The Economist* continues:

"To try to restore the privacy that was universal in the 1970s is to chase a chimera. Computer technology is developing so rapidly that it is hard to predict how it will be applied. But some trends are unmistakable. The volume of data recorded about people will continue to expand dramatically. Disputes about privacy will become more bitter. Attempts to restrain the surveillance society through new laws will intensify…".

"Yet here is a bold prediction: all these efforts to hold back the rising tide of electronic intrusion into privacy will fail… people will have to start assuming that they simply have no privacy. This will constitute one of the greatest social changes of modern times."

The editors conclude that, offered the choice, some might choose to reject even the huge benefits an information economy (supposedly) offers—"safer streets, cheaper communications, more entertainment, better government services…". But they will not be offered the choice and the cumulative effect of surrendering each bit of personal information will spell the end of privacy.

Almost simultaneously, Reg Whitaker, a York University political scientist, published his book, *The End of Privacy: How Total Surveillance is Becoming a Reality*. Whitaker recalls Jeremy Bentham's 18th Century panopticon (described in our 1996-7 annual report). This was a prison built with a central tower from which guards could observe the inmates around the perimeter, but the inmates could not see into the tower. The tower might be unoccupied but its visibility tricked prisoners into thinking guards were watching all the time, hence it assured "the automatic functioning of power".

Whitaker argues that new technology offers the potential for real as opposed to fake omniscience, replacing the one central panopticon—and its all-powerful inspector—with a decentralized panopticon with many inspectors. Each time we conduct a transaction that is recorded—and what transactions are not?—our data flashes across the network. "That momentary transparency aggregated with all the moments at which you are recorded …yield a unified pattern" Whitaker observes.

The new panopticon's strength is that we participate voluntarily, seeing only the obvious advantages—convenience, speed and personal safety—not the less tangible and more complex disadvantages. The most chilling of these is that we will conform because we assume that we are all being watched at all times. Put more starkly: freedom is diminished and, in some cases, disappears.

Welcome to the debate

These arguments may not be new, but their increasing frequency clearly signals a growing awareness that our heedless use of surveillance technology is having a profound impact on our society. To both *The Economist* and Dr. Whitaker I say I do not contest the possibility of your predicted outcome, but I do reject its inevitability. We still have a great deal of our privacy left to lose, considerable privacy to regain, and consequently much to protect. I heartily welcome you to the debate; it's about time this issue was taken seriously.

Defenders of a private life are often accused of interfering with an "open" society, as if freedom of information and a free press obliges everyone to live in metaphorical glass houses. Certainly government must be open and accountable to its citizens, allowing us to draw conclusions about the quality of government policy and administration. And the media has the right and responsibility to report on matters of public interest, guided (one fervently hopes) by a concern for accuracy and fairness. But there is no obligation in a

free society for individuals' lives to become an open book for government, the media, or their neighbours. Some evidently choose to bare more than many of us care to know—witness some prime time TV. But what we share about our lives, and with whom, are choices only the individual can make. Respect for one another's boundaries is the hallmark of free societies.

The argument that only the guilty have "something to hide" builds on the flawed notion that privacy is about keeping unpalatable secrets. Yet scratch even the most ardent advocate of unfettered technology and you will find a topic that triggers some reserve: personal finances, sexual preferences, medical conditions—we all have "something to hide" and a right to hide it. Truly these matters are no-one else's (or very few people's) business. Those who have had the misfortune to live in states that treat the individual's information as their own understand how this builds social control and weakens the individual.

Human values must drive the bus

Accusations that privacy advocates are all Luddites, or technophobes trying to forestall new technologies, assume we reject the new tools. It also

assumes that information technology must intrude. Both assumptions are wrong. Privacy advocates use and enjoy the technologies. We understand their appeal; they can be liberating and powerful. But that does not blind us to the flaws. Human values, not technology, must drive the bus. We can build privacy and data security into information technologies if we are determined to do so. The public sector appears ready; its chief informatics officers recently endorsed as a fundamental principle "that privacy is not an obstacle, but rather a significant element of any IM/IT project". Encouraging words indeed.

I believe that in the long run the doomsters will be proved wrong. The situation may get a good deal worse before it gets better—is bound to get worse if the current level of public apathy and ignorance persists. The pace and extent of the changes and society's attitude towards them is astonishing. In less than the term of a privacy commissioner, we have gone from media dismissal of some of our warnings as overheated and hyperbole to its supine conclusion that it's too late to fight.

The real problem is not the technology, or even some of its seductive promises of convenience, security and efficiency. It is our failure to comprehend the heavy costs that come with the benefits of technology's unchecked insinuation into every facet of modern life.

Trading our souls for loyalty points

It is hard for us, beset by the manifold problems of daily living, to be aware of the deeper, underlying currents of societal change. The immediate practical value of a price discount from a shopper's loyalty card is far easier to grasp than the long-term implications of the incremental collection of personal information. But each apparently trivial disclosure accumulates until our life history and pattern of living become available for use and misuse by the corporation and the state. We will have sold our souls for a few loyalty points.

Thus the real threat to privacy has never been the prospect of some cataclysmic event which would send us to the barricades. No, the threat is the gradual withering of our individual control of personal information and our passive or unknowing acceptance of the longer-term consequences. It is the death of freedom by inches, which history shows is most often the way that freedom dies.

The death-of-privacy arguments posited by *The Economist* (and, sadly, too often and too eagerly endorsed by legions of bureaucrats in government and business) boil down to this: we will eagerly exchange our freedom for the beguiling prospect of more security, efficiency and convenience. No longer is Big Brother watching you. As Dr. Whitaker put it "Big Brother is watching out for you". Technology in the hands of the state and the corporation becomes our master—and we its servant. We are effectively building ourselves an electronic Gulag.

Perhaps not enough people yet realize that privacy and freedom are inextricably linked; one cannot exist without the other. Those who doubt the proposition are invited to consider this: if you would measure the degree of freedom extant in a society, look first to the degree of privacy enjoyed by its inhabitants. The relationship is striking. Therein lies the explanation for the acute sensitivity of some European states such as Germany which, mindful of its own history, now is in the forefront of data protection.

But this failure to understand the link is pervasive and leads to many dubious notions taking root. Thus, a prominent columnist recently argued that a compulsory national identity card is the only answer to preventing fraud in immigration, welfare and health benefits.

Papering over the cracks

Disregarding the oft-experienced phenomenon that crooks will always find a way to beat the system, the proposal hits rock bottom in the evaluation of basic rights. Better that all should be regimented that the few miscreants might be caught. Or to put it more accurately, better that all should be put under surveillance than that bureaucrats and politicians be compelled to produce better and more enforceable administrative programs that do not require such draconian measures.

We cannot have fallen so far in our disregard for the preservation of core values integral to a civilized society: respect for the rights of others. But one would be naïve not to concede the existence of the threat.

The challenge, as always, is to awaken society to the problem, and there is ample evidence of encouraging signs. Several countries, Canada included, are taking steps already to strengthen the individual's right of choice and control of personal information. The European Community has already acted, many former Eastern European countries are doing the same. New Zealand, Hong Kong and Thailand have passed privacy protection statutes. Australia is

poised to follow. None can doubt that these movements reflect a growing public constituency determined not to let technology ride roughshod over basic rights.

Is privacy dead? Assuredly it is struggling, but struggle is the eternal and unchanging fate of all freedoms. Freedoms, once lost, can only be regained at the cost of great effort and pain. None can say with certainty that freedom will not be lost here. But if freedom survives at all, so too will privacy, because by definition freedom cannot exist without the right to a life free of surveillance and regimentation.

This struggle is far from finished. To paraphrase the American naval hero John Paul Jones, we have just begun to fight.

A Long Journey

Canada is arming itself with a new weapon for the fight. Our response to this electronic communications juggernaut is part principled and part pragmatic—principled in our determination to see vital human rights respected, and pragmatic in a desire to see the nation at the forefront of electronic commerce.

As Parliament rose for the summer recess, left on the table was Bill C-54—the *Personal Information Protection and Electronic Documents Act*. The bill is intended to extend the reach of federal privacy law into the commercial sector. (For a capsule guide to the bill, see page 89.)

Presuming it becomes law, the bill will take the most important step in defence of individual privacy since passage of the *Privacy Act* bound the federal government in 1982.

If it does not, Canadians can be forgiven for regarding business' handling of their personal information with a jaundiced eye—and electronic commerce with downright suspicion. Without the legal right to control how business collects and uses our personal information, our privacy on-line will be whatever the owners of the systems are prepared to concede—and if protecting it gets in the way of business, that could be precious little.

Rightfully, the bill has attracted a good deal of attention, and the Commons committee hearings stretched over several months. Representations fell into two main categories: business, which felt it was too rigorous—and consumer and civil rights groups who argued it was too gentle. Perhaps a good balance has been struck.

Although far from perfect (and what piece of legislation ever is?), in its essentials this bill is a long leap forward. When fully implemented, it would require business to respect a code of fair information practice requiring individual consent for the collection, use and disclosure of personal information. Equally important, it provides a mechanism for independent oversight—mandating the Privacy Commissioner of Canada to investigate complaints, issue reports and conduct audits. As a last resort, it provides recourse to the Federal court and empowers the court to award damages when it feels a penalty is justified.

The bill represents considerable ingenuity, and not a little courage. Most commercial activity in Canada falls under the jurisdiction of the provinces (the exceptions being banking, telecommunications and interprovincial transport). However, the federal government has the constitutional power to regulate interprovincial and international commerce. Thus the bill takes effect in two stages. The first stage brings federally-regulated business under the privacy umbrella, one year after its passage. Then, after three years, the federal law will apply to commercial activity inside provinces that fail to adopt comparable privacy laws of their own.

While undeniably sensitive, the government has acted to ensure that all Canadians, wherever they live, can look forward to a common standard of legal privacy rights.

A level playing field

Not incidentally, business wherever it is conducted, can breathe easier knowing that at the heart of the bill is the Canadian Standards Association's Model Privacy Code which the private sector helped create and over which it can claim some ownership. As someone put it recently, the Code has some "moral force" in the business community. The bill should help establish a level playing field, outlawing rogue information practices which could tarnish the rest of the private sector.

Equally gratifying is the government's decision to retain the ombuds role for complaint investigation. Some witnesses argued that a quasi-judicial, order-making commissioner would be more effective. Believing in the maximum of negotiation and education, and a minimum of heavy-fisted enforcement, we disagree. Our 15-year experience has proved the effectiveness of this model, 15 years in which the emphasis has been not only on resolving complaints but identifying and correcting the underlying problem.

If all else fails, the court is there. But of the 20,000 complaints we have handled since 1983, fewer than a dozen have prompted our seeking recourse to the courts. The office is less a police department than a problem solver. Our approach has always been non-confrontational and non-adversarial—one that will be even more necessary in the private sector. Business is a world of infinite complexity; crashing through its doors in a fashion either arbitrary or impatient would doom the cause of enhancing privacy observance from the start.

The bill's objective is not to impede business but to strengthen it, and to buttress the public's trust in electronic commerce. It is to help create a state of mind in which business routinely considers client, customer and employee privacy rights in developing products and administrative practice. Plainly, this is going to take time and patience. But there is no doubt that the end result will be extremely positive. Business depends—far more than government bureaucracies—on satisfied clients and customers. Its reputation is any company's most important asset, and no one will want to risk being singled out for wilful flouting of individual rights.

Fighting ignorance

One vital element of the bill is that it provides the office the tools to fight the single greatest privacy problem in Canada—ignorance. The office will be given a formal mandate to undertake public education. Business will need and is already welcoming our assistance. Consumers will want to know their rights and their responsibilities. The more people know, the less they fear and the more informed choices and decisions they can make. But no bricks without straw, as the saying goes. Vital as public education is, it demands resources, and this for an office that has struggled mightily with historic underfunding (and no funds at all for research and education). While the Treasury Board began addressing the problem in the past year, extending the office's mandate to the private sector will require substantially more straw.

Bill C-54 is no magic bullet. Many privacy problems remain. The appetite for surveillance continues to grow. All governments harbour many who argue that greater efficiency demands an unfettered flow of information from department to department, government to government, and business to government—and vice versa. Administrative efficiency sweeps aside all other considerations—including our right of informed consent to the collection and use of our personal information.

Perhaps *The Economist* is right; the laws now being considered or already enacted will not be enough to stem the tide of surveillance. Should experience prove that to be so, more will have to be done. If needed, more *will* be done. But we must begin by doing something and doing it quickly. If we fiddle in the face of lobbying and jurisdictional disputes, Canadians' privacy and the business opportunities on-line will burn.

Bill C-54–Some Observations

A number of criticisms have been levelled at the bill, some of them specific and technical in nature. Copies of our detailed commentary are available from the office and on our Web site. Among the criticisms are two that beg discussion here; the exemption for information gathered for "journalistic, artistic or literary" purposes, and for law enforcement.

The journalism exemption This one strikes a personal chord; readers are cautioned that these observations are coloured by more than three decades in journalism—the occupation many profess to despise but which almost all concede is indispensable to a free society. Consider Thomas Jefferson's famous remark that, forced to choose between a country with a government and no free press, and one with a free press but no government, he would unhesitatingly choose the latter. But no freedom is absolute, even in journalism.

Several questions were raised about the exemption during the bill's passage through Parliament; clearly some MPs believe that contemporary journalism is reaching unacceptable levels of privacy intrusiveness. The Commons committee questioned my support for this exemption, and I have often been challenged on privacy and the media.

Let's acknowledge a basic truth. The media are not in the business of protecting privacy. They are in the business of gathering and distributing news. However, they do have a responsibility to avoid needless harm by publishing or broadcasting material that serves no real interest beyond the prurient.

Journalists bear a weighty responsibility. Nothing is so precious to anyone as a good reputation. Reckless damage for no other real purpose than to titillate or entertain readers can have lifelong consequences. Even handsome financial compensation by the courts cannot retrieve a person's good name (and few have the resources to even contemplate court action).

The mainstream media in Canada generally do a pretty good job (although some in public life may disagree). Certainly there have been some notable and deplorable exceptions but there has yet to be the Canadian equivalent of the kind of media frenzy such as the ruthless harassment of the Royal family. Of course, public figures must expect a diminished level of privacy, and many welcome it since public attention is essential to their careers.

But subjecting journalists to a law that requires consent for the collection of personal information would cripple their ability to perform their job which, however occasionally unpopular, is so indispensable to a free society that it is recognized in our Charter of Rights and Freedoms.

Law enforcement exclusions Another exemption is worthy of comment. The law enforcement lobby in Ottawa has managed once again to persuade the government to give it unnecessarily broad exclusions from privacy law. Note that "law enforcement" includes not just police forces but those who administer such laws as the *Income Tax Act* or the *Employment Insurance Act.* The exemptions cast a cloak over all such investigations, meaning businesses may not tell someone that they have responded to police or bureaucrats' demands for personal information, unless the agency agrees. This is a sensible requirement so long as disclosure would have the effect of impeding or injuring an investigation. But once the investigation is finished there is seldom good reason for not telling the individual what has been done with the information, particularly in the case of administrative investigations.

However, Bill C-54 gives law enforcement agencies absolute discretion. They need not demonstrate an injury to their investigation in order to deny the individual access to the information. And, unlike the federal *Privacy Act*, there is no requirement to keep a record for the Privacy Commissioner. This obligation has proven to have salutary effects on federal agencies; it provides an audit trail for investigations.

On the other hand, businesses are not required to give up information merely on the say-so of a police officer. They are perfectly entitled in the absence of a warrant to decline to give information. And since warrants are not required for many administrative requests (although the form of request is usually prescribed), there is all the more reason to make the process accountable.

The most that can be said about unfettered police discretion to deny access to investigative files is that it is also to be found in the existing *Privacy Act.* We have objected to this discretionary power, and will continue doing so with greater vigour than ever. This issue sits high on the list of amendments needed to bring the existing *Privacy Act* up to date.

The need to amend the *Privacy Act* takes on a fresh urgency with the impending passage of C-54; the two acts contain some important differences that need to be reconciled. For example, the existing *Privacy Act* permits

recourse to the Federal Court only in cases of denial of access to records. Not included are complaints about collection, use or disclosure of personal information—the heart of any privacy code. Bill C-54, on the other hand, allows an appeal to the court for all such complaints. If this discrepancy stands, Parliament will have acquiesced in a lower standard of privacy protection for the federal government than for the rest of the country. That is hardly defensible.

The Health Infoway: Path to Health Surveillance ?

There is some progress on the health privacy front this year. Proposals to build a national health data network, first aired in the government's 1997 budget, offered exciting prospects for improving Canadians' health and the health care system. They also posed substantial privacy risks to patient data without stringent safeguards. As our 1996-97 annual report observed, "The prospect of greatly expanded collection and sharing of personal medical information sets privacy alarm bells ringing".

We have followed developments closely, meeting Health Canada officials, briefing members of the Advisory Council on Health Infostructure to keep privacy on the agenda, and providing them comments on the interim and final reports.

The Final Report—*Canada Health Infoway: Paths to Better Health*
In February, the Council issued its final report which seemed to acknowledge the critical importance of privacy, citing privacy protection as one of the four strategic goals to be met when building the network. It also recognized the important distinction between protecting patient privacy—which may mean not collecting some information—and ensuring that patient data is secure. The Council also supported specific health privacy legislation and identified the essential components of any such legislation. As well, the Council supported harmonizing privacy protection across all jurisdictions and specifically cautioned against sinking to the lowest common denominator.

All well and good. But some other important messages seem to have been lost. The first is the report's apparent failure to acknowledge the patient's right to choose not to participate in any health information network. Nor does it speak about limiting surveillance of individual patients who do participate.

The report's recognition that groups of people can be stigmatized by having health information used against them was another important milestone. Unfortunately the recognition was limited to Aboriginal and immigrant communities. Any group of individuals can be perceived as having particular attributes that are then ascribed—rightly or wrongly—to any member of the group. The conclusion can be simplistic and dangerous. The concept of

"group" privacy deserves broader interpretation in the health care context and more attention overall.

The report also gives short shrift to another of the Office's recommendations—that research and ethics review boards include privacy or patients' rights advocates. Without someone to speak for individual rights, the mantra of "public interest" or perhaps "greater efficiency" will inevitably win the day. Allowing health bureaucrats and researchers to represent the patients' interests risks putting Colonel Sanders in charge of the chicken coop.

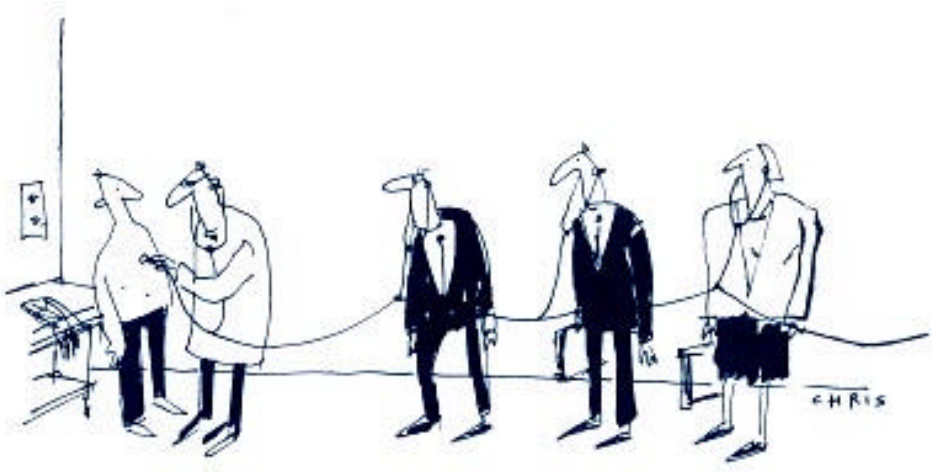
Fuelling our concern is the tone of the companion *Health Information Roadmap,* produced by Health Canada, Statistics Canada and the Canadian Institute for Health Information. If this document is intended as the blueprint for implementing the report, some important pages are missing.

The Health Information Roadmap The roadmap describes the steps needed to build a comprehensive health information system and infrastructure to deliver health care to individuals. While it acknowledges that "individuals have important rights over when and how their personal information is used", its answer to protecting those rights is patient access to privacy policies, and stripping names from the medical information. The first risks being mere window dressing; the second attempts to provide confidentiality, not privacy.

It's clear that patient privacy is at stake. Even the most sanguine would draw a breath at proposals in the roadmap to "follow the movements of individuals within the formal health care system over extended periods of time". Among its proposals is the need for more "person-oriented information"—as well as expanding the range of data collected. Among those "expanded data sets" are those on health status and the "non-medical determinants of health". The surveillance aspect of health information is most apparent in the proposal for a National Health Surveillance Network.

The National Health Surveillance Network Certainly there is a need to monitor selected situations and individuals to protect the public against such immediate hazards as infectious diseases or dangerous pesticides. However, the network's function now seems to be evolving into promotion of health and well-being. Advocates of population surveillance seem to be applying the substantial arguments for protecting against public health risks, to promoting health—a different kettle of very different fish.

The longitudinal tracking proposed in a Health Canada discussion paper—to whit, "of the entire array of socially determined roles, personality traits, attitudes, behaviors, values, relative power and influence that characterize the lives of men and women in Canadian society"—is breathtaking, intrusive and offends the bedrock value of privacy in a democratic society. Any health network must allow patients to opt out of such social surveillance without penalizing their health care. Once again, advocates seem to have confused good security with protecting privacy. Informed consent is too fundamental a privacy principle to be pushed aside.



The major weakness in the report, the discussion papers and the roadmap is the lack of detail on how the information will flow. There are no diagrams to explain how and where health information would be linked, the extent of individual detail, or who would have access. Without such detail, health providers, bureaucrats, patients and privacy advocates are unable to determine where the risks are and how to eliminate them.

In fact, the dearth of detail is itself a cause of argument among the players. For example, the Council has repeatedly protested that there is no plan for a single integrated patient case file. Yet the Health Information Roadmap talks about "an integrated health system where patients can move seamlessly between hospitals, long term care, home care, and other settings depending on their needs", and "an integrated patient record (at the regional or local level)". The roadmap goes on to speak of collecting "more detailed data on

specific groups or individuals" and "working with all provinces to enable a potential *pooling* (their emphasis) of information held in their person-based record systems".

One would be hard pressed not to conclude that the Health Infoway proposes a massive integration of personally-identified patient profiles, nationally accessible to a broad range of care givers, researchers and bureaucrats. It is small comfort that health network advocates say they are not creating "centralized databases" of patient information, but "distributed networks". This is a distinction without a difference. Whether the data is gathered in one central repository or accessible on-line through the network, it will be widely accessible. Its protection will hinge on the number and rigor of the controls on access. Protecting patient "privacy" by replacing patients' names with identifying numbers is a simplistic solution to a complex problem. It is a simple matter to re-identify the individuals and so unlock a comprehensive and intensely detailed profile. And who else will line up to argue that they need access—law enforcement officials? Social welfare agencies? Employment and pension bureaucrats? Pharmaceutical companies?

While we can accept that the work is in its early stages, and that the infrastructures vary from one province to another, it seems inconceivable that the various projects could have progressed to this stage without some attempt to chart the information exchanges. The denials are contributing to a growing aura of suspicion around the project. It's time the officials laid out the specifics and allowed the source of all this valuable data—the individual patients—to participate in the policy debate.

Legislators looking for guidance on health information privacy law need not re-invent the wheel; the Canadian Medical Association's Health Information Privacy Code is a comprehensive benchmark for achieving a high national level of protection for patient information. The code could be the basis for drafting legislation. Given the grumblings that the code sets the bar too high, perhaps some

Health Infoway funds should be used to study the impact of its implementation. The patients at the heart of this system deserve no less.

Saskatchewan's Health Information Law

Saskatchewan's new *Health Information Protection Act*, which received royal assent in early May, makes the province's health information practices more transparent and gives patients some control over their personal health information. As one local journalist put it, "there's something fundamentally comforting that Canada's birthplace of socialized medicine is now also the first province to enact an individual's right to withhold comprehensive personal health records from government bureaucrats, even if the right must be exercised in a pro-active way".

Some of the principles in the preamble were drawn from (among other sources) the Canadian Medical Association's Health Information Privacy Code. Patients can choose not to have personal information they confided to their physicians stored on the Saskatchewan Health Information Network or any prescribed network. As well, the patient may require a "trustee" (i.e.: any person of body that has control of health information) to restrict other trustees' access to all or part of the information on the network. And section 9 requires trustees to promote patients' knowledge and awareness of their rights under the act.

The offences for violating the act send the right message. For example, anyone convicted of "unlawfully obtaining" personal health information can be fined up to $50,000, and $500,000 if the crime is committed by a corporation.

But there are some causes for concern. For example, the definition of trustee is very broad; almost anyone could qualify. No distinction is drawn among doctors, government institutions or companies providing health services through an agreement with another trustee. In addition, the act doesn't apply to statistical or so-called "de-identified" personal health information. De-identifying information (by substituting a code, for example) is a far cry from making it anonymous—by definition, de-identified information can be "re-identified" as long as the system can link the information to a patient.

There is also a lengthy list of secondary purposes for which patients, personal health information can be disclosed without their consent. These include if

there is a danger to the safety of anyone, not just the patient, or to "monitor" or "reveal" fraud, or for oversight committees to monitor service quality. Significantly, the government has given itself considerable flexibility through broad regulation-making powers throughout the act.

So while we are cautiously optimistic about the protection the legislation affords patients, several questions remain. For example, what criteria will be used to determine who can be a trustee? And will the research ethics committee include privacy or patient rights advocates ?

Getting Serious about SIN

Auditor General confirms SINs' shaky foundations

Readers of earlier reports will know that uses and abuses of the now infamous Social Insurance Number (SIN) elicit more than the Office's passing interest—and sometimes predictable yawns from others. The sides of the debate are drawn between those who see expanded SIN use as the slippery slope towards integrated databases and a national ID card—and those who dismiss the fears as an irrational response to a national file number.

SINs' greatest threat has always been its potential to become a national identifier and thus a powerful key to personal information in increasingly interlinked information systems. This is a serious threat from a number which is treated so cavalierly by government, business and individuals alike.

The most recent, and arguably most forceful, recognition of the SIN problem comes from perhaps a surprising quarter—the Auditor General. For the Privacy Commissioner to say SINs are a problem is hardly news. But when the Auditor General, with his harder-edge mandate (and the resources to probe extensively), concludes that the management of the number courts risks of fraud **and** privacy intrusions, alarm bells rang.

Admittedly, not all the A.G.'s recommended solutions sit well with a privacy commissioner—government economy and efficiency are the A.G.'s focus, after all. But we are grateful that the number and its supporting system are finally getting the rigorous attention they deserve.

The Auditor General's probe assessed "the management and control of SIN to determine if it is efficient and effective and has an appropriate base in legislation".

He concluded that SINs has become "a de facto national identifier for income-related transactions, contrary to the government's intent". Despite government moves to limit its own uses of SIN following Parliament's three-year review of the *Privacy Act*, the 1992 amendments to the *Income Tax Act* swung the door open wide. Amendments required SIN on social assistance and workers' compensation payments.

"This virtually guaranteed the dominance of the SIN as the common program identifier for provincial and municipal social programs", concluded the Auditor General. When coupled with federal social programs, the A.G. calculated the total government social program expenditure at almost $100 billion a year. When "almost any transaction related to an income support payment or loan, revenue collection, and an individual's personal finances has a SIN attached to it", there is huge incentive for data linkage. Even when the estimated rate of fraud ranges between one and four per cent, the possible payback may be just too tempting to policy makers—sufficient to sweep aside the ethical niceties and remove the legal barriers.

The A.G. also found about 3.8 million more SIN holders in the Social Insurance Register than there are Canadian residents age 20 or older. This calls into question the accuracy of the supporting database. It also opens the doors to that growing threat in an information society—identity theft. And the new Canada Education Savings Grant is expected to add an estimated one million children to the ranks of SIN holders—even though there are no tax consequences for children until they actually begin drawing from education savings plans.

Improve the Register Three of the Auditor General's recommendations demand a privacy commissioner's response. First is the need to improve the integrity of the register. The A.G. suggested tightening up the proof-of-identity requirements for all new SIN applicants, demanding—for example—that an eligible guarantor sign the application, rather like a passport. He also proposed a cross check with provincial vital statistics branches to verify birth certificates for new applicants, as well as cull the names and numbers of those who have died. Unreported deaths are thought to be the major cause of the millions of excess numbers.

Obviously the register needs a housecleaning. How to go about it? Once the almost definitive proof of identity, sadly birth certificates are now apparently inadequate. Since they are sometimes forged, the information now seems to demand confirmation from the issuing jurisdiction. All well and good if it is simply to confirm the bare facts. Not so good when the vital statistics registry itself may contain gratuitous detail such as those reportedly found recently in the Alberta registry. The details, included information about the mother's lifestyle (tobacco, drug and alcohol consumption).

These details might satisfy bureaucratic curiosity but they do nothing to improve the SIN registry's accuracy. The example highlights the critical importance of restricting any such federal government access to the bare details needed to validate the identity of applicants and to remove the deceased.

Another major contributor to the excess of SINs over people is the 900 series—those "temporary" SINs beginning with "9" issued to non-permanent residents (such as refugee claimants, seasonal workers and foreign students). By 1998, 680,000 of these were active—66 per cent of them more than five years old. Many SIN holders may simply not have notified the registry that they have left the country; others may be in the country illegally. The A.G.'s suggestion to issue 900 series SINs with an expiry date seems both fair and logical in the light of their temporary status.

More problematic is the proposal that the registry have access to the client files of Citizenship and Immigration to confirm the person's status, and to Revenue Canada to verify that a number is active. We can accept the need for Citizenship and Immigration to alert the registry to any change in a client's status—becoming a landed immigrant, being deported—but not the registry routinely trawling through immigration files.

Nor can we accept the registry gaining access to the files of any government agency using SIN to determine whether particular numbers are active. The danger posed by such broad access is that the register will gradually amass details on the holders' transactions. That data would transform the register from its primary function into a data matching clearing house.

A more accurate register and tighter proof of identity would go a long way towards correcting inaccuracies and preventing fraud and abuse.

Imbedding identity verification features in the card The A.G. also argues that the card itself needs more information to confirm that the person producing it is its legitimate holder. Among the options offered are photographs, digital signatures and biometric identifiers such as retinal scans or hand geometry.

This is the dangerous point at which the SIN mutates from client file number to a bone fide identity card—a step any privacy commissioner must resist.

Identity cards, even those designed for specific purposes, tend to develop noxious secondary characteristics. Even when the card is not necessarily required to receive a service, producing one quickly becomes part of the service routine—and then becomes mandatory. Not having one, or simply not carrying it, becomes sufficient grounds for suspicion and probable denial of service.

The card, perceived as accurate and secure, gradually assumes an importance of its own. Other government organizations in search of reliable identification climb aboard. Gradually and inevitably it becomes a government identity card. With that kind of cachet, the private sector soon joins the chorus demanding the card. And what we have created, in effect, is an internal passport. Without one, you are nobody.

A further consequence is that with such a reliable identification, the use of SIN will likely grow. Expanded use increases the danger that government and business can access your information wherever it is held, without your knowledge or consent. More users and increased access lead inevitably to bringing more information together with the attendant risk of profiling. And with detailed profiles comes the spectre of organizations predicting, manipulating and coercing individual behaviour.

All these risks are compounded by the vacuum in law which imposes few limits on who may ask for and use your SIN.

While it is difficult to argue against a more accurate and secure card, perhaps a more immediate and practical question is how useful it would be in the millions of transactions that Canadians routinely conduct at a distance; filing an income tax return or applying for Canada Pension Plan, for example. Arguably these transactions form the vast majority of our contacts with government. The weakness of the SIN is also its power; it can be used (and misused) by mail, over the telephone and perhaps one day—on line. Imbedding security features on the card itself will be little help.

We support the A.G.'s call for tightening the original identification process for issuing SINs, and asking for additional identification when processing in-person transactions. As the A.G. put it, "let him who is with SIN show another piece of identification". A more rigorous screening of new applicants could increase trust in the numbers. But what about the 33 million already in circulation?

Policy and legal reform Canadians are poorly armed in the face of growing pressures to allow greater sharing of personal data. Using SINs to collect personal information from all authorized users could lead to detailed and invisible profiles of individuals. All the current abuses of SIN would be exacerbated. Detecting and preventing misappropriation of public funds is a worthy cause but not one that justifies putting citizens in electronic straitjackets. There has to be a better way.

Government could begin by following the advice it has been given consistently for more than 15 years—set out in law who may ask for the number and how they may use it, then forbid other uses. And provide for sanctions against those who breach the law. Government cannot contemplate expanding or formalizing the number's use without putting it in a legal framework.

Nor should SINs be used to expand information sharing until government spells out in law specific rules on data matching. The *Privacy Act* is silent on the practice and the Treasury Board policy on data matching seems more

honoured in the breach than the observance. The Auditor General stresses the need to clarify the rules and the roles of the parties in asserting control and accepting responsibility. Having repeatedly urged the same, the Privacy Commissioner can only applaud.

However, one reservation seems overwhelming—the Auditor General's report underscores how compromised the SIN has become. Is this the foundation on which we should build any new system?

Beyond the Numbers : the larger question

Last fall, following release of the Auditor General's report, two Parliamentary committees examined the SIN—the Standing Committee on Human Resources Development and the Status of Persons with Disabilities, and the Standing Committee on Public Accounts. Neither committee sought to duplicate the Auditor General's work. Both concluded that improving SIN's current administration was only part of the issue—the larger question was what government sees as the future of the SIN. "Resolution of the SIN mandate is essentially a political issue", concluded the Public Accounts Committee "that will require a decision from the Parliament of Canada".

In its report *Beyond the Numbers*, the Human Resources Committee supported several of the Auditor General's recommendations to improve current administration. However, despite extensive hearings, the committee concluded that it had not had enough time to study the crux of the matter—"the overarching policy issues of privacy protection and data matching—central to the future of SIN in Canada".

But another committee, the former Standing Committee on Human Rights, had examined those issues in its comprehensive report *Privacy: Where Do We Draw the Line?* The 1997 dissolution of Parliament eliminated the government's need to respond. Rather than lose the critical work, the Human Resources Committee adopted the privacy report in its entirety and has asked the government to respond formally to its recommendations.

Among the Human Resources Committee's own recommendations were several aimed at the broader context. The committee urged government to draft a bill setting out the legal uses of the SIN and providing penalties for misuse. This recommendation echoes those of Canada's first three Privacy Commissioners—and Parliament's own three-year review of the *Privacy Act.* After almost 20 years, it's not a moment too soon.

The committee set three immediate deadlines. It asked HRDC to report by September 30 on progress implementing the 1998-99 workplan to improve its SIN administration, which this office will review. Also by September 30, HRDC will table with the Privacy Commissioner its evaluation of a pilot project to update SIN data from New Brunswick vital statistics records. It will also consult other provincial and territorial governments about similar transfers (which the committee recommended that appropriate privacy commissioners review). The Commissioner in turn will review the New Brunswick project report and the department's recommendations, and table his comments with the committee within 30 days.

By December 31, the committee also asked the department to report on options and associated costs for "improving or replacing" the SIN with an entirely new card system. This is the crux of the matter. As the committee put it, "too many decisions about the current use of the Social Insurance Number were made by default". To contribute to a spirited and informed debate, the Privacy Commissioner anticipates tabling a position paper on identification card systems with the committee.

Committing a Social Science*

That 1911 Census…

News that the 1911 census returns would not be made public travelled like wildfire through the historical and genealogical research communities. One of the parties blamed was the Privacy Commissioner and the letters and e-mail descended.

It is true that the Privacy Commissioner has serious reservations about Statistics Canada promising absolute confidentiality for census information, then releasing the results through the National Archives. Following his investigation into complaints about the 1992 census, the Commissioner suggested destroying the personally-identified returns to deal with growing public concern over the increasingly intrusive questions—particularly those posed on the long form. While Statistics Canada has no need for the personal returns—the information has all been verified and entered into electronic data systems (without names)—the National Archives balked at destruction of the returns.

But the Commissioner's reservation is not the immediate reason Statistics Canada is refusing access to the 1911 census. In fact, the *Privacy Act Regulations* allow the National Archives to release census and survey results 92 years later for "research and statistical purposes". The barrier to access is the *Census and Statistics Act* of 1906 and several subsequent laws, all of which prohibit Statistics Canada from disclosing personal census information to anyone—including the National Archives.

The motivation for such stringent protection is clear: the law requires us to answer census questions. As society becomes more complex, the questions become more detailed, more sensitive and arguably well beyond those of a head count. Among the questions on the last census were those about personal wealth and income, religion, fertility, and physical and mental disabilities. The test version of the 2001 census includes a question on same-sex partners. And before each census, governments, academics and special interest groups line up to seek ever more information.

---

* with apologies to W.H. Auden

There is no arguing that census data is a huge and valuable resource for modern government and business. But when citizens are forced to disclose personal data under compulsion of law, government bears a heavy responsibility to protect the information. Failure to accept that responsibility courts the risk that individuals will refuse to answer, and damn the consequences, or that they will fabricate responses and corrupt the data. Successive governments have acknowledged that the trade of information for confidentiality is a fair one and have accepted their responsibility. The result is closing the census to public access.

The step is certainly not without precedent. Australia, a country with similar history and an equally healthy appetite for genealogical research, destroys its personal census returns to protect privacy—and the census bureau itself from pressures for unrelated uses.

Unfortunately, the sustained lobbying appears to be having some effect. The Industry Minister has asked Statistics Canada to develop options for amending the legislation to allow access to census records. According to StatsCan, there are two possibilities. The first is amending the *Statistics Act* to allow access to the 2001 and all subsequent censuses. The second is amending the act retroactively to override the confidentiality provisions under which all censuses beginning in 1911 were gathered.

Neither option is attractive. The first risks compromising the census process if substantial numbers of Canadians object. The second would break the legal promise Parliament made to Canadians in 1911—and every census year following. It would demonstrate to Canadians the fragility of government promises in the face of an organized lobby. That would be as undesirable as the intrusion into private lives. The Privacy Commissioner cannot support either.

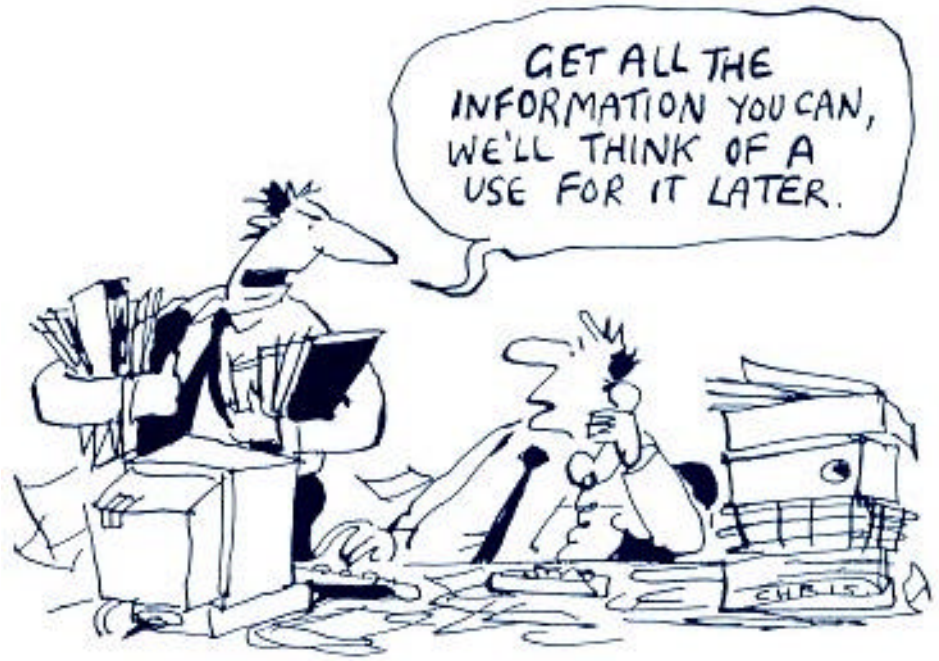
And Now for the "Survey of Financial Security"

If an indication were needed of Canadians' growing frustration with—and resistance to—government probing, Statistics Canada's "Survey of Financial Security" was a graphic illustration.

Once again, the survey prompted controversy including a public statement from one provincial privacy commissioner who observed that he would not participate if approached. Many of the issues in this survey are similar to those the office has dealt with when investigating similar surveys such as the

Family Expenditure Survey (see 1997-98 annual report)—the "intrusiveness" of the questions, the security of the collection process and any possible disclosures of the information.

The subject matter—finances—is always a sensitive one, and the depth of the questioning is more than some can tolerate. The 68-page survey is a comprehensive look at a household's finances, conducted through personal interviews in about 21,000 households. Its stated intent is to determine how well Canadians are coping financially.



To answer the broad question, the survey collects information about each individual household member with personal identifiers attached. The survey questions range from family composition—education, employment status and experience and physical and mental disabilities—to fine details about expenses, savings, assets, retirement benefit plans and how they manage personal finances. Among the questions to hit nerves were those asking whether the respondent had terminated a relationship with someone formerly in the household (within the past 1 ½ years) and why, whether each is a union member, and the registration numbers of their pension plans. The

survey also sought permission to examine the individuals' income tax and Canada (Québec) Pension Plan files.

However, two concerns were new; a statement in the interviewer's package that federal and provincial privacy commissioners had been "consulted" about the survey, and the low profile given to the voluntary status of the survey. The consultation with this office amounted to a telephoned alert of Statistics Canada's intention to conduct a survey, followed by a meeting to "review" the material about two weeks before researchers went into the field. The meeting was essentially a formality—all the material was printed and ready for distribution.

Privacy staff emphasized the need for the process and the options to be made clear to respondents. These included explaining to them that the survey was voluntary, that they could complete the questionnaire themselves (rather than in the presence of the researcher), and that individuals could have their own survey form if they wished (individual forms can be important in households of unrelated individuals). Staff also questioned keeping personally-identified survey responses, reiterating the office's position that destroying any personal links is a fair trade for collecting the very sensitive data it was seeking.

Statistics Canada staff insisted that its researchers had been specifically instructed to tell respondents that the survey was voluntary, and to respect a decision not to participate. They agreed to consider the other representations. Following the meeting, staff reviewed all the written material and found that the introductory letter to respondents said nothing about participation being voluntary. Also the accompanying brochure was somewhat opaque on the point. The briefing material for interviewers was far clearer and privacy staff suggested incorporating the language into the respondents' brochure. It was far too late in the process. Nevertheless, StatsCan agreed to change the letter to make the voluntary nature of the survey clear. It was the most we could hope for at the end of the process.

Shortly after interviewers went into the field, it appeared that even this change had not been made. Called for an explanation, StatsCan advised that regional directors have discretion to determine the wording of the letter to respondents in their region. At least two decided that making it clear that the survey was voluntary would reduce participation. They eliminated the statement.

Canadians must know why their personal information is being collected, how it will be used and disclosed—and their legal obligation to provide it. These are the core principles of the *Privacy Act.* These are not discretionary rights which government staff can set aside on a whim when they prove inconvenient to their administration.

The Commissioner is investigating complaints about the survey.

On the Hill

Proposed new laws or government programs often look both desirable and simple on their face. Who could possibly object to a national organ donor registry, or improving pre-clearance procedures at airports, or better detection of money laundering? The intent is usually laudable. It's only when the details start to emerge that so do the complications. Several cases in point arose last year.

Amending the *Proceeds of Crime (Money Laundering) Act*

In May 1998, the Solicitor General issued a consultation paper on amending the act to improve police ability to investigate money laundering. The proposals included obliging financial institutions to report suspicious transactions, proposed new enforcement measures and offences, and establishing a new federal agency to receive and manage the information.

Any law requiring financial institutions to report selected customer transactions to a government agency is a *de facto* intrusion into individuals' privacy. Detecting financial crime without abandoning individual rights is the challenge. The Office expressed its reservations with the proposals in a letter to the Solicitor General. Those reservations concern compliance with the Charter and the *Privacy Act*, defining a "suspicious transaction", the danger that reporting may violate professional privilege—and foster a climate of citizens informing on one another, and the structure and mandate of the new federal authority.

The department issued its Summary of Consultations on February 1, 1999, and Bill C-81 was introduced on May 31. Shortly before Parliament rose for its summer recess, it passed the amendments, some of which dealt with some of the Office's concerns. In the interests of alerting public, policy-makers and legislators alike, we repeat our reservations here, accompanied by the measures in the law.

Compliance with the Charter

Our reservations: Requiring organizations that provide financial services (such as banks, investment brokers and life insurance companies) to gather confidential client information for law enforcement agencies, without a warrant, could offend Charter protections against "unreasonable search or seizure".

The new law: The Solicitor General's department was also concerned about the Charter implications. Its response was to require law enforcement agencies to obtain a judicial warrant before seeking **additional** (our emphasis) information from the new federal authority. While this introduces some independent oversight into the process, it does not deal with the Charter implications of the initial collection of the information by either the financial institution or the federal authority.

Compliance with the *Privacy Act*

Our reservations: The *Privacy Act* requires institutions to tell individuals why they are collecting personal information and how it will be used. Notification is waived only when informing the person would compromise the accuracy of the information or prejudice its subsequent use. The proposed regulations do not address the individual's right to be told. Prohibiting financial institutions from telling their clients that they must report particular transactions may help identify relatively unsophisticated criminals; it is unlikely to fool sophisticated money launderers. Arguably a general practice of public notification is a useful public education tool.

The new law: The new law specifically binds the federal authority to the *Privacy Act.* However, it is unclear how that will meet the government's obligations to notify individuals at the outset about the collection and possible uses of their financial information. The problem remains that the data will be collected on the federal authority's behalf by private sector organizations not subject to the *Privacy Act.* Under this scheme, clients could only determine that their financial institution has disclosed their information by seeking access from the federal authority.

Defining a "suspicious transaction"

Our reservations: It was unclear whether the $10,000 threshold suggested in the paper, or any one—or combination—of indicators deemed "suspicious", would be sufficient to trigger the financial institutions' obligation to report. The danger was that financial institutions, in an effort to avoid exercising discretion (and possibly incurring liability), would resort to the monetary threshold alone. This risked forcing disclosures of substantial numbers of innocent transactions. We suggested that any legislation should require a combination of some other evidence with the monetary limit before triggering a report. Whatever the indicators, they should be evident on the face of the transaction and the immediate material circumstances. They should not require financial institutions to probe

substantially into the financial affairs of a client or any associated third party before deciding that the transaction is "suspicious".

The new law: The amendments make it clear that the financial threshold alone should not be the determining factor. Financial institutions must gather additional details (to be specified in regulations) before deciding that a transaction is sufficiently suspicious to warrant reporting. While a substantial step forward, the Commissioner would prefer to see a public debate on the matter rather than the invisible process of regulation-drafting.

Professional confidentiality

Our reservations: Application of the reporting requirements to "persons engaged in a business, profession or activity in the course of which cash is received for payment or transferred to a third party (e.g., lawyers and accountants)" could have violated the common law principle of solicitor/client privilege.

The new law: The law exempts lawyers from the reporting if doing so would breach solicitor/client privilege.

The federal authority

Our reservations: The authority will be responsible for analysing information it receives from institutions and individuals required to report under the act. It will also gather information from public sources, foreign law enforcement agencies, informers and the Canadian Police Information Centre. Note that all this information will be gathered without a warrant. However the authority's precise status is not clear. Although apparently neither law enforcement agency nor investigative body, it seems to fulfil both functions to some degree. Its status is vitally important because that will affect the application of the *Privacy Act* to the personal information it collects and holds. Will individuals have rights to have access to and correct information or will it all be denied because it was obtained during a lawful investigation? Will the authority's collection, use and disclosure of personal data be subject to legal limitations? Will individuals be told? Will there be independent oversight of the authority's operations? The discussion paper is silent.

The new law: Amendments have not clarified the authority's status. Is it an investigative body or law enforcement agency? The answer is critical because of its impact on the authority's ability under the *Privacy Act* to gather

information without individuals' knowledge and consent, and routinely block their access to it.

Our reservations: Once the authority has gathered and analysed substantial information—and concluded a transaction is "suspicious"—it would alert law enforcement officials. Since the federal authority collected the original information without a warrant, the authority's notification should be as limited as possible. Any further information should only be disclosed in response to a warrant.

The new law: The law limits the information the authority may disclose initially to law enforcement agencies. The details include the client's name, financial institution, the amount of the transaction and its form—(i.e.: cash, bonds, shares etc.). Any further disclosures require a warrant which would specify what additional information the authority must disclose.

Our reservations: Nevertheless, the risk remains that simply by identifying a transaction as "suspicious", the authority has supplied law enforcement agencies with sufficient grounds for a search warrant. This could lead to routine search warrants in response to the authority's notices.

The new law: It remains unclear whether the authority's notice will itself constitute "reasonable grounds" for the issuance of a warrant or whether the court would require additional information to satisfy the "reasonable grounds" test.

Building an Organ Donor Registry

Another example of trying to do the right thing but needing to dig a little deeper is proposals for a new organ donor registry. The House of Commons Standing Committee on Health studied ways of improving Canada's low rate of organ donation. Among the early suggestions was a possible national donor registry. The Committee sought the Commissioner's advice on the privacy issues it should consider before recommending setting up such a registry.

The value of a donor registry is readily apparent but collecting potentially sensitive information and storing it centrally demands a sound justification. With no resources to conduct an in-depth examination, the Commissioner

could only offer some preliminary observations. He suggested the Committee consider several questions.

Is there a sound justification for collecting the information and storing it centrally?
The Office is often confronted with assertions that the collection, use or disclosure of certain personal information about Canadians will advance some public interest, facilitate government operations or help law enforcement. We have become increasingly reluctant to accept these assertions at face value, particularly given the lack of sound evidence behind many of the proposals, and the inherent privacy intrusions the collection entails.

What information would the proposed database contain?
Would the information simply indicate a person's willingness to become a donor, plus contact details—address and telephone number—or would it include all relevant medical information such as blood type and genetic makeup? If any personal medical information were to be included in the database, what security safeguards would protect the information from unintended access and disclosure?

Would the information be used for any purpose other than matching organs and tissue?
One recurring problem with databases in Canada is that, established for one purpose, their use gradually expands beyond those intended at the time of the original collection. As a general rule, any unrelated secondary uses of personal information should be prohibited unless the individuals provide their express, informed consent. A database intended to facilitate organ donations should not be used to further some other government program, such as law enforcement.

To whom would information in the database be disclosed?
If the database is intended to facilitate organ donations, the information it contains should not be disclosed for any other purposes unless the individual expressly consents. There are too many instances of information being collected and used in the public interest, then disclosed for much less acceptable purposes.

Is it appropriate to create the registry by obtaining consent on federal income tax returns?
Government used this method to gather addresses for the permanent voters' list. While that was justified on grounds that an up-to-date accurate list is vital to a well functioning, healthy democracy, an organ registry might not pass a test of similar general public necessity. How many more worthy

causes could make the same claim, and what would that do to the income tax return?

The Commissioner offered to discuss his reservations with the Committee. However, the Committee's report (issued in April 1999) took a cautious approach, concluding that a national registry of intended donors would not be the most efficient use of resources. The Committee recommended establishing national lists of those awaiting "solid organs" (such as heart etc…), actual donors, and potential donors in hospital. It also suggested a national database to track the results of organ donations using the Canadian Organ Replacement Register. All of these suggested lists are more focussed on both the individuals and the medical procedures at stake and are far preferable to a comprehensive national database.

The Committee's findings and recommendations served as effective reminders to consider signing that organ donor card.

Convenience has its cost—pre-clearing U.S. Customs

Efforts to speed air travel between Canada and the United States (and enhance Canada's appeal as the gateway for international travel to North America) prompted the government to introduce legislation authorising American officials at major Canadian airports to clear travellers for entry into the U.S..

Pre-clearance would allow Canadian travellers to clear formalities at the beginning of the trip, then fly to any U.S. destination, rather than being restricted to those with customs and immigration services. International travellers could cut flight times by routing their flights through Canada, without having to obtain Canadian visas or pass through Canadian Customs en route to the U.S.. This enhances the international appeal of using a Canadian carrier.

Bill S22, the *Preclearance Act*, is intended to formalize a Canada/U.S. agreement allowing U.S. customs and immigration officers to clear incoming Canadian visitors or in-transit international travellers at Canadian airports. The government will not enact the bill until the 1974 agreement has been amended to guarantee reciprocity. The advantages of the procedures are undeniable but there are some wrinkles.

The bill would allow U.S. officials to screen travellers for customs, immigration, public health and food regulations. It would expand their current powers from simply refusing entry, to searching (a "pat down"), seizing goods and imposing fines. U.S. Customs officers could not arrest anyone, only hand over suspicious individuals to Canadian authorities. Although the powers are not new (customs officials have been clearing travellers under the 1974 agreement), this is the first time they have been written into legislation. Effectively, the bill allows officials of a foreign power the right to gather information on Canadian soil. It has prompted substantial concern about the extra-territorial application of U.S. law, and the protection offered by Canadian law on Canadian soil.

One of the laws in question is the federal *Privacy Act.* All border-crossing procedures gather personal information. Entering another country is a privilege; complying with the country's entry requirements is a given. But the information is usually gathered in the host country and governed by that country's laws. Since the bill moves some of the data collection into Canada, will Canadian privacy rules apply?

The Department of Foreign Affairs assures us that "all use of personal information will be consistent with Canadian privacy law and policy". The bill includes specific references to the *Charter* and the *Canadian Human Rights Act.* And it is clear that once someone is detained and handed over to Canadian officials, Canadian privacy law applies. But the statement begs several questions: Will individuals have a right of access to, and correction of, information collected by U.S. officials? Could they challenge its collection, use and disclosures? And if so, with whom—who could passengers ask to review U.S. officials' handling of personal data collected on Canadian soil to administer a U.S. law?

For passengers in transit through Canada, U.S. officials would also collect "behavioural" information or profiles. This data could include the city where the trip started and any other cities visited, gaps in the trip, when the ticket was purchased, how paid for and by whom, the name of the travel agent, seating and dietary preferences, and any phone numbers given. The international airline would transmit the data to U.S. authorities in Canada to run against profiles of suspicious travellers. Those matching the profiles may be targeted for secondary examination and may be denied entry. U.S. law provides no review of this decision.

Canadian customs officials are not authorised to use profiling to make administrative decisions about travellers. By allowing the practice on Canadian soil, this agreement would seem to lay the groundwork for Canada Customs using the technique—one the Privacy Commissioner finds unsettling and that Canadians have so far resisted. Is this Parliament's intent? All told, it is difficult to accept government's claim that the bill is "consistent with Canadian privacy law and practice". It is ironic that the bill recognizes the paramountcy of the *Canadian Human Rights Act*, which first established Canadians' privacy rights, but not that of the expanded *Privacy Act*.

Senate Committee calls for drug testing transportation workers

In June 1998, the Senate struck a special committee "to examine and report upon the state of transportation safety and security in Canada". In its January 1999 interim report, the Special Senate Committee on Transportation Safety and Security called on the government to permit mandatory, random drug and alcohol testing in the Canadian transportation industry similar to that required under United States legislation.

No one could oppose measures to enhance transportation safety in Canada. The Senate Committee made several sound recommendations to this end. However, we are troubled by the Committee's ready acceptance that drug testing is necessary and that it will enhance transportation safety.

The office has examined drug testing on several occasions. Each time, the question returns: does broad and random testing do the job? The drug test itself is intrusive, it cannot reveal impairment, and the information generated by testing is both sensitive and subject to misuse. Given its intrusiveness, drug testing should be required by the state only where there is compelling evidence of its need.

There is precious little evidence that many of the forms of drug testing so eagerly embraced by governments and the private sector, and so keenly marketed by the drug testing industry, enhance workplace safety. In the majority of cases, the only appreciable impact of drug testing is a serious diminution of the fundamental human right of privacy. Too often, drug testing does little more than strip people of their dignity—and their constitutional rights—on the basis of flimsy assertions that drug testing "works".

In a detailed study *Drug Testing and Privacy*, 1990, the Commissioner made several specific recommendations about broad testing programs. Among them was the recommendation that "random mandatory testing of members of a group on the basis of the behaviour patterns of the group as a whole may be justifiable only if the following conditions are met:

- There are reasonable grounds to believe that there is a significant prevalence of drug use or impairment within the group;
- The drug use or impairment poses a substantial threat to the safety of the public or other members of the group;
- The behaviour of individuals in the group cannot otherwise be adequately supervised;
- There are reasonable grounds to believe that drug testing can significantly reduce the risk to safety, and
- No practical, less intrusive alternative such as regular medicals, education, counselling or some combination of these, would significantly reduce the risk to safety.

Nothing in the intervening years has altered our view that such sweeping testing is unwarranted. The Commissioner has asked for an opportunity to appear before the Committee to discuss his concerns.

Reviewing the Corrections and Conditional Release Act (CCRA)

The CCRA is currently undergoing a five-year review by the Standing Committee on Justice and Human Rights. Early in 1998 the Solicitor General sought public input in its consultation paper *Towards a Just, Peaceful and Safe Society*. Since inmates retain many of their rights, any discussions about amending the CCRA should be done with the *Privacy Act* in mind. This is not a matter of either/or—not only can the *Privacy Act* and the CCRA coexist, they can complement each other.

The Privacy Commissioner's comments focussed on four issues:

The relationship between the CCRA and the *Privacy Act:* Although the CCRA provides inmates many of the same information rights as the *Privacy Act*, it does not provide independent review of complaints. Thus an inmate who has received personal information under the CCRA may then attempt to make a complaint to the Privacy Commissioner about inaccurate information. Correctional Services Canada and the National Parole Board have argued that inmates only have rights to correct information obtained under the *Privacy Act.* This forces them to make a formal privacy request for information already in their possession. This is bureaucratic at best. Parliament should amend the CCRA to indicate that any information provided under that act is deemed also to have been provided under the *Privacy Act*.

Urinalysis provisions: The submission reiterated the comments set out in our 1992 paper. Drug testing is highly intrusive and although inmates have a reduced expectation of privacy, they should not be deprived of a fundamental human right to any greater degree than is necessary. Drug testing should not be used unless it can be demonstrated that it reduces both the use of drugs in institutions and the incidence of violence.

The Solicitor General argued in 1992 that drug testing would do both yet the latest consultation paper provides no such evidence. In fact, there is some evidence that inmates may be switching to harder drugs that are more difficult to detect by drug testing. Thus there has been a significant

expansion of drug testing in institutions without any evidence that it is achieving the promised results. We understand that CSC intends to study the matter; we await the results with interest. It is vital that drug testing not lead to a change in drug use that fosters the spread of HIV, hepatitis and other blood-borne infections.

Offender information: The consultation paper observes that there have been some problems with sharing inmate information between CSC and NPB. We are comforted that the *Privacy Act* has not been fingered as the culprit. Both the *Privacy Act* and the *CCRA* contain sufficient provisions to allow CSC and the parole board to share the information needed to fulfil their responsibilities.

One caution concerned the concept of integrated justice. Any additional sharing of personal information within the justice community must abide by the relevant privacy legislation and we urged that federal, provincial and territorial privacy commissioners be consulted at the earliest possible point.

National Parole Board Registry: An apparent clash between public accountability and individual privacy can often be resolved by sensible compromise. A case in point could be (but is not yet) the National Parole Board's Decision Registry.

Several complaints from parole applicants cited the extensive details the Board revealed in its "decision sheets" which any interested party could examine in the NPB Decision Registry. The complaint investigations revealed, in some instances, considerable psychological and counselling detail and, in one case, financial information. The Commissioner considered some of the disclosures excessive and the complaints well-founded. He wrote to the Board.

Since then the Board has held training sessions with Board Members (who write the decisions) and its staff on the relationship between its own enabling statute (which requires public disclosure), and the *Privacy Act* which gives parole applicants access to their own information but protects it from third parties.

The result has been generally shorter decisions and a greater focus on only the details that are relevant to the parole decision.

We have no difficulty accepting the Board's need to account publicly for its decisions to put offenders back on the streets before their sentences are completed. And we acknowledge the improvements that are evident from the ongoing training. However, the problem remains that the Board is trying to kill two incompatible birds with one stone—explain the Board's decision to the applicant and be accountable to the public.

The decision "sheets" are more than a single page summary of the decision and the factors that influenced the Board's decision. They are the Board's written decision from the hearing and the record that the applicant receives. The information could include psychological or counselling details, or information about family members and other third parties—all of which the applicant should see.

In fact, the Decision Registry is "virtual" only. There is no data bank containing the Board decisions. When a member of the public asks to see the decision "sheet", the Board decision is pulled from the applicant's file. Thus the sheet attempts to serve two purposes; providing the applicant the maximum information possible about the Board's decision while not going overboard in disclosing details to the public. The conflict of interests is too great to be reconciled in the bosom of one document.

The Commissioner recommended the Board create an actual and discrete public registry containing summary information about the applicants, the decisions and a synopsis of the reasons that led to the decisions. This would meet the Board's obligation of public accountability. Then Board members could provide parole applicants with a detailed document explaining their decisions without risking excessive public disclosure.

The Board rejected the recommendation, one of several made in the Office's submission to the Solicitor General on the review of the *Corrections and Conditional Releases Act.* The legislation is currently before a Parliamentary committee.

The *DNA Identification Act*

The Senate passed the *DNA Identification Act* without amendment, but not without reservation, in December 1998. The act requires the Solicitor General to establish a national data bank of DNA profiles taken from crime scenes for use in criminal justice investigations. More important in the context of privacy, it will also contain both actual DNA samples and DNA

profiles of those convicted of "designated offences"—generally, crimes involving violence. The RCMP Commissioner will maintain the data bank.

The act is the second phase of legislation dealing with the use of DNA in criminal investigations. The first phase, allowing the forced taking of DNA samples from suspects under a warrant, was enacted in 1995.

The Commissioner put several concerns before both the House of Commons and Senate Standing committees reviewing the bill—with mixed results.

Parliament rejected our recommendation that the legislation not allow keeping the actual DNA samples taken from convicted offenders, rather than simply the analysis, or profile, of the DNA sample. The danger of storing the physical samples is the temptation it offers future governments to authorize further testing for completely unrelated purposes.

To deal with its reservations, the Senate Legal and Constitutional Affairs Committee obtained several undertakings from the Solicitor General. Among them were

- Creation of an advisory committee, including a representative of the Office of the Privacy Commissioner, to oversee implementation of the act, and administration of the DNA databank. The committee urged the Solicitor General to include the appointment of the advisory committee in the regulations.
- Publication of the regulations before they take effect, allowing the Senate time for evaluation and comment.
- Agreement to clarify in regulations what is meant by a "DNA profile". The regulations will specify that a DNA profile is "not a profile for medical reasons". This will restrict police use of profiles to identifying individuals for law enforcement purposes, and not for predicting medical, physical or mental characteristics. This clarification helps address the Senate Committee's (and our) concern about the dangers of storing the samples.
- Consideration of a provision for Parliamentary review every five years given the highly sensitive nature of the information and the rapidity of technological change.

As we go to press, we understand that the Solicitor General is developing a mandate for the advisory committee. We will seek to ensure that the committee is indeed independent, and will participate in its work as fully as our resources allow.

A close watch on the DNA provisions in our criminal law is absolutely essential. There is already considerable pressure in other jurisdictions to increase substantially the number of individuals whose DNA would be captured for criminal investigation purposes. Canadians will almost certainly face such pressures in the near future. Unless they resist, they may find, as is now being seriously considered in Britain, that all citizens, innocent or guilty, may be required to surrender their DNA for the alleged advancement of crime control—and the certain surrender of privacy.

Issues Management and Assessment Branch

The Issues Management and Assessment Branch monitors government programs and legislation, researches emerging issues, and provides the Commissioner policy advice and communications support.

A handful of portfolio leaders provide the Office a contact point with federal agencies to resolve issues before they lead to complaints. This pro-active approach has been the focus in the past year, replacing formal audits and follow-ups.

The branch also depends on a few policy analysts and researchers to keep the Office current on any other developments that concern privacy. This includes examining new legislation and government programs, and researching developments in Canada and abroad to help develop positions on specific issues, and to provide background for the Commissioner's public appearances.

Branch staff also help handle some of the more complex questions that fall outside the mandate of the Commissioner, providing inquiries officers with input on selected subjects. They act as contact point for international data protection commissioners on privacy protection in Canada and support the Investigations Branch, providing information and obtaining expert advice as needed.

Much of the research and expertise that helps the Commissioner prepare for his public communications has always originated in the branch. This year the branch assumed responsibility for both communications and Parliamentary liaison. This change has allowed the Commissioner's public communications efforts to become more focused and responsive to emerging privacy issues. In particular, this change has helped to support the Commissioner in the Office's heightened profile as a result of Bill C-54. Any of the branch's resources not consumed by the above have been devoted to monitoring the progress of this bill.

In addition to following the Health Infoway, new legislation and SIN issues discussed above, the Branch monitored the progress of several other issues including privatization of government agencies, a video surveillance policy, and preparations to renew the Canadian Police Information Centre.

The St. Lawrence Seaway transfer—getting it right

The recent spate of government privatization seems to have abated. Once a source of considerable concern—clients and employees were effectively losing their privacy rights—privatization has moved down the list of privacy threats.

Two factors have reduced the threats. The first should be the passage of private sector law for the federally-regulated private sector. Virtually all of the agencies that have been commercialized are in sectors under federal regulation and so should be covered by Bill C54, the *Personal Information Protection and Electronic Documents Act*.

The second factor is a growing understanding and acknowledgement by privatized organizations of the need for (and the benefits of) a major housecleaning of personal files. Purging the files of unneeded information, and obtaining employees' consent for transferring the remainder, can pay dividends. Employees are full participants in the process and the organization can often shed tons of paper.

One of the last agencies to be privatized was the St. Lawrence Seaway Authority. Perhaps understandably, the authority's personal records transfer was smooth and rigorous. Several months before the November 1, 1998 transfer date, the authority committed itself to continue respecting the principles and guidelines of the *Privacy Act*. Although most employee information is kept by the authority's human resources services, senior management instructed supervisors to review their working files for employees' personal records. They set out the broad categories of records, appropriate retention periods and what should be destroyed or sent to human resources.

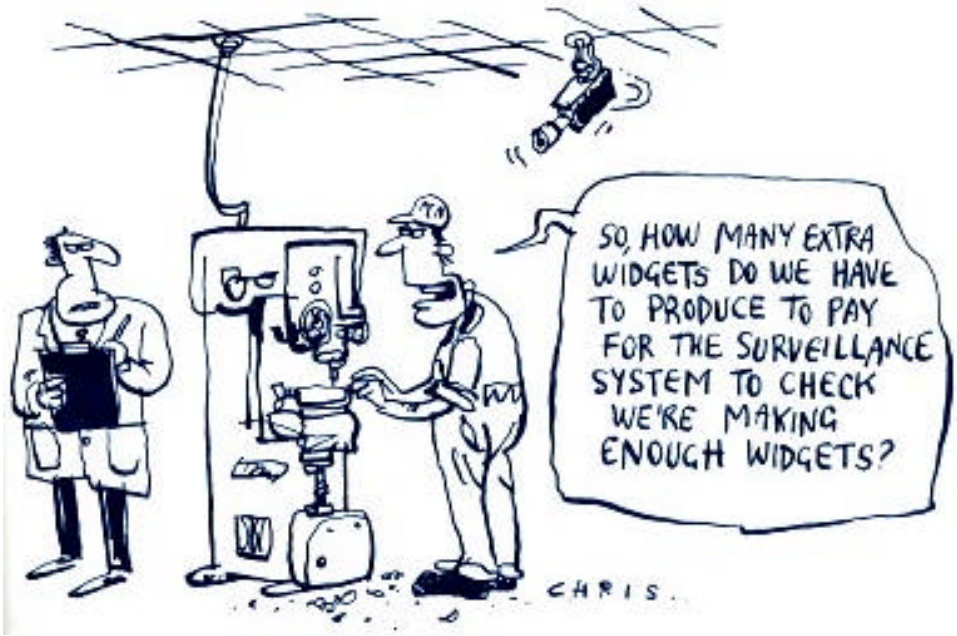
Management then wrote to all employees being transferred, explaining what information would be required to continue pay and benefits, and to honour collective agreements and employment claims. The letter then listed what other personal information the authority held and sought the employees' consent for the transfer. Employees could consent to transfer all, some, or none of the information with no adverse impact on their employment at the new agency. Supervisors were then told what was not to be transferred and required to sign a written confirmation that the records had been destroyed.

The whole process was relatively painless and demonstrated yet again that good privacy practices are good information management practices. What new organization would not want to get that right—from the beginning?

Complaint prompts video surveillance policy

Last year we reported an employee's complaint that Immigration and Refugee Board had planted a camera in the ceiling above her desk because they suspected her of leaking information from board hearings. The Commissioner concluded that IRB's evidence was so scant that it should have conducted a thorough preliminary investigation before resorting to such intrusive surveillance. Disturbed by management's quick recourse to a concealed video camera, the Commissioner wrote urging the Treasury Board to draft a government-wide policy on covert employee surveillance.

In April 1999, Treasury Board issued a Security Policy Implementation Notice to all departments in an effort to guide security staff on using cameras during investigations. Citing both individuals' *Charter* rights to a reasonable expectation of privacy, and their specific rights under the *Privacy Act*, the notice sets out all the requirements based on those set out in the Commissioner's 1997-98 annual report.



The notice requires that any policy on covert video surveillance "take into account the following:

- reasonable grounds to suspect serious misconduct, which may include criminal misconduct, must exist before covert video surveillance is considered an investigative option;
- any decision to conduct covert video surveillance necessarily raises substantially more privacy concerns than overt video surveillance and should only be considered when all other reasonable measures, including non-investigative measures such as counselling, workplace notices, education programs and overt surveillance, have proven ineffective or are likely to prove ineffective;
- do not use where individuals have a reasonable expectation of privacy (for example, a private office, change rooms or a single office in an open office environment). If the alleged conduct under investigation is believed to be criminal, police should be asked to investigate. This will ensure a court review since police must first obtain a warrant to conduct covert video surveillance where there is a reasonable expectation of privacy;
- where individuals do not have a reasonable expectation of privacy (e.g. public access and reception areas), authority to order covert video surveillance should rest only with a senior level official with the advice of the departmental security officer and departmental legal; in ordinary circumstances, the deputy head should be informed in advance of any covert video surveillance being conducted;
- to the extent possible, covert video surveillance should not intrude on the privacy of persons other than the individual under investigation;
- the surveillance should not continue longer than is reasonably necessary to conduct the investigation;
- access to the videotape and any information generated by the videotape should be strictly limited to those with a need to know and should not be used, for example, as a vehicle for monitoring employee performance generally. The videotape and all information gathered in the course of the investigation are subject to the *Privacy Act*, *Access to Information Act*, and the *National Archives of Canada Act*;

- the individual placed under covert video surveillance should be notified afterwards about the surveillance, including where and when it occurred, and the justification for the surveillance, unless there are compelling reasons not to do so."

CPIC Renewal

In April 1999 the Solicitor General announced funding to modernize and renew the Canadian Police Information Center (CPIC), the computerized information system for Canadian law enforcement. CPIC is a cooperative, managed by the Royal Canadian Mounted Police and shared by municipal and provincial police forces. Other agencies such as Canada Customs and Correctional Services Canada have restricted access.

CPIC managers have always recognized that this system maintains and provides access to a large volume of personal information and have a rigorous privacy code in place. Since the redesign will also have to address the privacy issues, project managers seconded an experienced staff member from the Privacy Commissioner's Office for the duration of the project.

On the Stump

In addition to the Commissioner's appearance before Parliamentary committees on impending legislation (reported earlier), he and staff spoke to more than a dozen audiences ranging from Dalhousie University law students to a group of unemployed persons in l'Estrie, Québec. Copies of speech texts are available from the Office or on the Web site.

Senate Committee of the Whole Certainly the most notable invitation of this or any year was a call for the Privacy Commissioner to appear before the Senate Committee of the Whole. The opportunity was somewhat akin to briefing one's board of directors. The Privacy Commissioner is among a tiny band of Officers of Parliament—those appointed by and responsible to Parliament to defend fairness, decency and honesty in public administration.

While once commonplace, the practice of calling witnesses before Committees of the Whole "appears to have gone out of fashion", the Commissioner observed. Acknowledging that efficiency may be the reason, "…one baneful result in my view has been a reduced public visibility of the legislative process, and of the workings of government."

The Commissioner gave a brief privacy State of the Nation then dealt with Senators' questions and comments on everything from his defence of keeping census returns private, to the proposals for U.S. Customs pre-clearance at Canadian airports.

New Thai Constitution Enactment of Thailand's new Constitution gave the Office an unparalleled opportunity to share what it has learned—and is still learning—with a country just introducing information law. The Thai Constitution contains several mechanisms designed to increase government transparency and accountability, including a human rights commission, ombudsmen and administrative courts. One of the most critical is the (then) Office of Information to administer the *Official Information Act.*

Under the Canadian International Development Agency's Governance Program, a senior Office manager was invited to Thailand to describe the Canadian experience with information law. The manager first spoke to the Prime Minister's nationally televised conference on the new law in May 1998, then participated in several meetings of officials tasked with setting up the new information office. Following the visit, the office was renamed the Office of Information Access and Privacy Protection and privacy was given a prominent place in the decisions of the information commissioners.

The Thai office's director and two other senior officials then visited Canada for a first-hand look at administration of the *Privacy Act* and the *Access to Information Act*. The Office's manager returned to Thailand several months later to address the first anniversary conference on some of the lessons Canada has learned—and some it has not. He gave a lecture to a local university and met staff of the Information Office and government departments, focussing on the practical demands of implementing the law—identifying information holdings, preparing administrative handbooks and designing training courses.

The experience reinforced for Office staff how critical information rights are for a democracy, and how often Canadians take them for granted—or dismiss them outright.

Crossing Boundaries: Privacy, Policy and Information Technology Early in 1999, the Privacy Commissioner and staff participated in a series of roundtables sponsored by the Institute of Public Administration of Canada (IPAC). The four roundtables brought together Members of Parliament, senior public servants, journalists and academics to discuss the tension

between a "public service which favours better and more information in the service of better government" and citizens' concerns that this could "lead to a more intrusive or authoritarian state". The debate is a classic one and, as IPAC observed, "dialogue would help".

The first roundtable set the context, the second examined privacy and the changing role of government, the third looked at integrating data across jurisdictions, and the fourth at sharing between government and the private sector.

There are many to speak for "efficient" government; so many, in fact, that one wonders how government became so inefficient. The roundtables took as given that "integrating information systems and data bases allows government to function more efficiently and effectively"—an assumption that itself may be flawed. More information does not mean more knowledge. Far fewer echo what the U.S. Supreme Court observed was the role of the American Bill of Rights. The court described that role as to "protect the fragile values of a vulnerable citizenry from the overbearing concern for efficiency that may characterize praiseworthy government officials no less, and perhaps more, than mediocre ones".

In his presentation to the second roundtable, The Commissioner underlined the role efficiency should play in government—and of the role of law in protecting the individual against its too enthusiastic pursuit.

IPAC expects to issue a comprehensive report of the proceedings later this year.

Investigations and Inquiries Branch

Incoming complaints jumped past the 3000 mark for the first time in the office's history—new complaints reached 3105 for the 1998-99 fiscal year. Two factors contribute to the heavy intake, one of these is complaints about government matching of returning travellers' customs declarations with employment insurance claims (see page 84).

A second factor was more than 225 complaints of delays by Correctional Services Canada staff at the Cowansville (Québec) Institution. Employees filed more than 900 requests to see their personal records during a contract dispute. To help reduce the paper burden, CSC made appointments with employees to examine their files rather than receive copies. The *Privacy Act* permits examining originals and, in the circumstances, is reasonable in the face of employees using the act as a tool during labour disputes.

Two other departments that have struggled to meet the time limits, now appear to be making significant progress. National Defence and Revenue Canada reorganized their ATIP sections into work teams early in the fiscal year and the efforts are paying dividends. By the end of the reporting year, the pace of their time limits complaints had fallen off remarkably. Other departments take note.

Cases

The following selected cases illustrate the types of complaints the Privacy Commissioner receives.

Divorce registry procedures streamlined
A Manitoba lawyer's complaint about the Department of Justice's sharing his name and address with Human Resources Development Canada (HRDC) led to changing the way divorcing parties are advised about splitting Canada Pension Plan (CPP) credits.

The lawyer complained that Justice had improperly disclosed his name and address to HRDC's Income Security Programs Branch. (He also complained that HRDC had improperly collected the information from Justice.) The disclosure stemmed from a routine monthly transfer of computer tapes from Justice's Central Registry of Divorce Proceedings to HRDC. The tapes contained the names and addresses of those filing for divorce (or their

lawyers') provided by provincial courts for the Divorce Registry. Justice maintains the registry to detect duplicate divorce applications.

The privacy investigation revealed that in January 1993 Justice amended its Registration of Divorce Proceedings Form to collect the mailing address of divorce applicants or their legal representatives. Justice did not need the addresses for the register; it collected them solely to help HRDC send information packages to applicants about splitting CPP credits. (Couples divorcing after 1987 are legally required to divide equally any CPP credits accumulated by both parties during the marriage.)

The court registrar completes the forms and, when the application is filed, sends Part 1 to Justice to issue a clearance certificate. Once the court has disposed of the case, the registrar completes Part 2 and sends it the registry (non-personal information is also sent to Statistics Canada). The court keeps Part 3.

The registry is considered public. When only the lawyers' names appeared (to protect those leaving abusive relationships, for example), the procedure led to lawyers becoming mail drops for multiple copies of information packages for their clients which essentially duplicated information the lawyers may have already provided. As the complainant put it, "I may have the responsibility to my clients to advise them about their rights to apply to divide CPP credits, but how I choose to honour my professional responsibilities is not the affair of Health & Welfare Canada"(the department formerly responsible for CPP).

The arrangements failed several privacy tests. It was evident that Justice was not collecting the information for its own legally mandated program but rather was acting as an agent for a third party, HRDC, which is legally responsible for administering the CPP. Nor was Justice collecting the information directly from the individuals concerned but from the provincial courts. Direct collection generally ensures greater accuracy, and gives individuals the opportunity to give (or refuse) consent. Finally, Justice was disclosing to HRDC—and HRDC was collecting—unnecessary information about the divorcing parties' legal representatives.

The procedure also did not necessarily protect against abusive spouses. During the investigation, a woman filed for divorce and asked the court not to inform her husband until after she had left the country. The court agreed but the information was sent routinely to Justice, transferred to HRDC and

the husband received the information kit before his wife could leave. Apparently she was not harmed but the incident encouraged the departments to first delay the disclosures by two months or more, then find a new procedure.

The complaints also raised the question of why a personal communication was needed at all; generic information on splitting credits should be sufficient and much more cost effective; HRDC was mailing about 100,000 kits annually at a cost of approximately $500,000.

Both departments acknowledged the privacy problems and undertook to fix them. However, given the importance of ensuring that divorcing parties understood their rights and responsibilities for splitting pension credits, they intended continuing the procedure until they found an acceptable solution. The Privacy Commissioner considered the complaints well-founded but held the files open while monitoring the departments' pursuit of a solution.

In January 1999 Justice instructed the courts to stop collecting the addresses of the divorcing parties on the Registration of Divorce forms, effective February 1. Once the stock of old forms is exhausted, the replacement will not ask for addresses. Although the database will continue to include the address field (which would be costly to remove at this point), there will be no information to enter. The field will be removed during a proposed future redesign of the system.

HRDC took our point that information on pension splitting need not be personally addressed. It has now produced a fact sheet, explaining CPP credit splitting rights, which it provides Justice for distribution to provincial courts. The court simply adds the fact sheet to the envelope containing the divorce judgement. An added benefit: HRDC anticipates substantial cost savings from the new scheme.

Volunteered DNA samples and analysis destroyed

A complaint that appeared routine on its surface touched an issue which the Office has pursued since 1996; destruction of DNA samples volunteered during police investigations. Although the complaint itself was not well-founded, it contributed to the Commissioner's efforts to have the RCMP establish a national policy to destroy volunteered DNA samples (and any analysis), once the volunteer is eliminated as a suspect.

The Commissioner has consistently urged police to destroy volunteered DNA samples. In fact, he is not at all comfortable with asking people to "prove their innocence", a procedure which stands our legal process on its head. Nevertheless, those who do volunteer to help police investigations deserve stringent protection.

The case stemmed from an RCMP investigation of several sexual assaults in Vermilion, Alberta, in 1996. As part of its investigation, the local RCMP detachment asked approximately 400 males in the community to volunteer samples for DNA analysis to match against evidence from the crime scenes. There was considerable community pressure on men to comply.

The complainant, a Vermilion resident who had first refused, then reluctantly provided a blood sample, subsequently sought access to information about the DNA sample in RCMP files. He also wanted to know whether the information was in any other DNA databanks under provincial or federal control.

The RCMP refused access because it gathered the information while acting as a municipal police force in Vermilion. The *Privacy Act* prevents the force from disclosing any information it gathers while "performing policing services for a province or municipality" if the province or municipality asks for confidentiality (subsection 22(2)). Four provinces, British Columbia, Saskatchewan, Manitoba and Nova Scotia, have waived confidentiality in these cases, allowing individuals to seek access under federal law.

This puts complainants in a Catch 22 situation—although Alberta has a broadly similar privacy law covering provincial operations, the province argues that its law does not cover the RCMP even when providing provincial or municipal policing services. Effectively the personal records are out of the reach of any interested applicants unless provincial authorities give the RCMP permission.

When the man's request arrived at RCMP's Ottawa headquarters, privacy unit staff asked the Vermilion detachment for the information. The detachment advised that the sample had been destroyed. Rather than simply telling the applicant so, the RCMP then refused him access to the information citing the policing exemption. The man then complained to the Privacy Commissioner. However, the issues in this case reached beyond denial of access—to the RCMP's right to keep the information at all.

The Commissioner's investigator spoke to the police officer who had no objection to the man knowing that his sample had been destroyed and that he was not a suspect. This should have resolved the complaint—the man could get the information he wanted, the Commissioner would know that the information had been destroyed, and the RCMP would maintain the legal exemption. However, the RCMP advised that it would continue invoking the exemption. Office management then intervened with the RCMP, which agreed to have its investigating officer tell the man what had happened to the sample.

But, more important, was the police officer's confirmation that while the sample had been destroyed, the autoradiograms (the visual representation of the sample) computer printouts, work notes and lab reports would remain on file until a suspect was tried and convicted. The RCMP Commissioner wrote to confirm that the material is not put in any electronic database; however, it does become part of the overall investigative case file which is used "as required for disclosure, court and appeals".

It appeared that a volunteer had fewer rights that someone whose sample had been obtained by warrant (and therefore with some grounds for suspicion). It is RCMP policy to destroy a DNA sample obtained under warrant—and the analysis of the sample—once the person is eliminated as a suspect.

Neither the complainant nor the Commissioner was happy.

The Commissioner wrote again to the RCMP Commissioner, reiterating his position on volunteered samples and seeking a consistent national policy on their destruction. The complaint was held open. Several meetings, telephone calls and e-mails later, and following on-again-off-again notices of destruction, the RCMP confirmed that *all* the man's information had been purged. But it would still not tell the applicant so.

Frustrated, Office management asked the Alberta Department of Justice to waive its confidentiality agreement with the RCMP in this case, allowing the police to confirm for the complainant that all the information had been destroyed. Alberta agreed.

Finally, in August 1997, the RCMP amended its operational policy to require that "voluntary samples of bodily substances and the resulting DNA

information will be destroyed if the innocence of the contributor is established".

Although the Commissioner considered the complaint not well-founded (because legally the RCMP is prohibited from disclosing provincial and municipal policing information), its impact was substantial. Both the RCMP and any future volunteers can take some comfort from the resolution—a reassurance that DNA samples and analysis which establish their innocence will not find their way into police files.

The cases remain unsolved.

Employment insurance investigators examine old passports—and a good deal more

An added wrinkle to the continuing saga of the Customs-EI datamatch (see page 84) was a complaint by a Québec man that an employment insurance (EI) investigator had obtained his expired passport from Foreign Affairs to track his trips out of the country.

This was just the tip of the iceberg. When the EI investigator was notified of a February 1995 "hit", she asked for a credit report from Equifax from which she determined the man had credit cards from three banks. She faxed requests for information to the banks and received detailed listings of credit card purchases for the period. The reports identified payments to travel agencies and purchases made outside of Canada.

Following another hit on a December 94-January 95 trip, she asked two travel agencies for information about any trips they had arranged for the complainant. She also faxed Foreign Affairs, asking for his expired passport. The Passport Office sent the passport, asking the EI investigator to return it to the complainant, once she was finished with it.

The immediate question was why Foreign Affairs had an expired passport; normally they are voided and returned to the traveller. According to the Passport Security Section, the department keeps passports when they are seized abroad, when they are issued but not picked up, when they are used to illegally assist aliens abroad, and when a new passport is issued before the old one expires. (Apparently some countries require travellers to hold a passport three to six months before they enter.) How long Foreign Affairs holds a passport would depend on which of the circumstances apply.

There was nothing unusual in the complainant's computer file to explain why it was kept. The file indicated that a new passport had been issued and the old one cancelled.

Foreign Affairs staff could not explain why it instructed HRDC to return the passport to the man once the EI investigation was finished. It was evident that Foreign Affairs staff had not followed its policy of channelling all such investigative requests though its Access and Privacy (ATIP) unit. ATIP staff used the incident to remind passport staff to follow the procedure. A more important question was whether it was wrong to disclose the passport to HRDC. The Commissioner concluded that Foreign Affairs was faced with a request citing broad investigative powers in another act of Parliament. They could not be faulted for giving up the document.

Whether HRDC should have matched its EI database with returning travellers' Customs declarations—the process that led to it gathering all the information—is the issue now before the Federal Court.

Lost birth certificate just tip of iceberg

A Montreal lawyer complained to the Commissioner that the Immigration Refugee Board (IRB) had not only denied his client access to her personal information but also not returned her original birth certificate. The investigation revealed several problems, not just with the original request, but with IRB's handling of its records.

The lawyer asked for any correspondence and notes from the refugee claim officer concerning authentication of his client's birth certificate. The woman had applied for refugee status and IRB began an informal hearing (an accelerated process). When IRB decided to have her birth certificate authenticated by Citizenship and Immigration Canada (CIC), it advised her that this would mean reverting to the regular hearing process.

After several months passed, the lawyer asked what was happening. The officer confirmed that he had sent the birth certificate to be authenticated. The lawyer then submitted the formal privacy request. IRB provided the 26-page refugee claimant file but found nothing in the officer's files. The file did not refer to the original birth certificate. The lawyer found it hard to believe that there were no relevant records and lodged the complaint.

The investigator had many discussions with both staff of IRB and CIC, all of whom maintained that verification was still underway. IRB insisted the birth certificate had not been returned. Shortly afterwards, during the hearing, the birth certificate was returned—it had been found in one of IRB's files. Frankly suspicious, the investigator asked for access to all the original files to track the path of the found birth certificate. IRB produced two files, a master file for the presiding member of the hearing, and a duplicate set. The files contained no notes, no administrative information or tracking activities. However, they did contain a memo from CIC declaring the birth certificate fraudulent—the memo was almost a year old. There was no authentication report and no indication of where the original had gone.

Other problems surfaced during the investigator's review. Apparently the case had been transferred to another claim officer more than a year before but no one told the investigator. Prior to the transfer, the claim officer had

purged the file of notes and comments that could prejudice the refugee's claim when transferred to another officer. This made it impossible for the investigator to confirm whether relevant information had been in the file that might have been germane to the original request.

The original officer denied knowing that the birth certificate had been found and returned to the owner, nor could he explain how it could have happened. Some of the problems seem to have stemmed from his having set up his own informal process of having CIC authenticate documents. Since he had no tracking system in place, he had accumulated several original IDs which he could not match to their rightful owners because he could not read the language.

The Commissioner agreed that the complaint that access was improperly denied was well-founded. He was particularly concerned about IRB's practice of routinely destroying staff's handwritten notes and observations. Whether an organization should retain notes can be determined by their intent. If notes are used to make an administrative decision—in this case, to determine whether a refugee claim should be accepted—they should be retained. Not to do so removes critical information from the reach of the individual and violates their privacy rights.

The Office is continuing to follow the matter with IRB to ensure it takes corrective action.

National Defence casts solicitor/client cloak over entire Board of Inquiry

One of this year's cases illustrated the problem the Office encounters when organizations cast legitimate exemptions far too broadly. A case in point was National Defence's use of the solicitor/client exemption (section 27) to refuse a Force's member access to the entire proceedings of a Board of Inquiry into the complaints.

The member had a lengthy dispute with National Defence (DND) over its handling of allegations of medical neglect and harassment. The complainant made repeated access requests for medical information and had been given volumes of material including, at one point, an opportunity to review the entire file. But as the dispute escalated, the member filed a redress of grievance which included a substantial monetary claim against National Defence.

Given the size of the claim, the department treated the grievance as a claim against the Crown. It established a Board of Inquiry to gather evidence, a process that ran parallel to the grievance procedure. The member was called to appear, then sought access to the Board file (about 2300 pages). DND denied all the records because, it argued, the Board's entire proceedings—except the findings and recommendations—were protected by solicitor/client privilege.

The Commissioner could not accept this broad an application of the exemption. The proceedings were a fact-finding exercise, not unlike an administrative investigation. Disclosing the information would not reveal any of the Crown's strategy or analysis or privileged information between the department and its solicitors. It seemed inherently contradictory for the complainant to be called to testify before proceedings over which the "other side" then cast a blanket of solicitor/client privilege. And if the complainant decided to pursue civil action, much of the material would have to be disclosed.

Lengthy negotiations ensued. The Office asked National Defence to use its discretion to disclose all the factual records and withhold only those consisting of legal advice. DND argued that there was a legal precedent that waiving solicitor/client privilege over one document meant effectively waiving privilege over everything. Seemingly at an impasse, the Commissioner wrote to the Deputy Minister.

DND rejected the Office's contention that the process was an administrative hearing to ensure a harassment-free workplace and a safe and healthy work environment. The member had been relieved of military duties for some years and was being released for medical reasons. Rather than seeking to improve the working environment, DND argued, what the member wanted was substantial compensation for the alleged mistreatment. The Board was constituted to gather "evidence that will be useful in instructing the Crown solicitors and counsel" about the validity of the member's claim. "The information was necessary to provide a legal opinion as to the Crown liability and ...form an integral part of the litigation brief", the DM wrote.

Nevertheless, DND agreed to provide copies of the member's own testimony and all those dealing with harassment, as well the medical file and other material already received. DND agreed to waive solicitor/client privilege over the vast majority of the Board's proceedings to settle the case.

How did they get my name? Rule out Canada Post

That perennial question we demand of our mailboxes got no satisfactory answer in one case despite the willing cooperation of everyone from Canada Post, the Canadian Direct Marketing Association (CDMA), list brokers and a direct marketer.

An Alberta university student who had seen the Privacy Commissioner on CBC's *Coast to Coast*, wrote about some curious mail his grandmother received from California. In Edmonton attending law school, the student had addressed some of his mail to his grandmother in Calgary using a Ukrainian term of endearment. The address included neither her given nor family name. About two years later, his grandmother began receiving quantities of unsolicited mail from California addressed to her correct given name but substituting the term of endearment for her family name—the equivalent of "Mary Grandma"!

Since only he and close family members used the term, and his grandmother certainly never referred to herself formally that way, the student concluded that only Canada Post could have been the source. The investigator went on the trail of the mail.

Canada Post denied scanning names and addresses on mail. First it does not have the equipment to record the information of everyone receiving mail. And, second, the information gathered would have no value for either the post office or direct marketers—the individuals would be such a large and undifferentiated group that they could not be effectively targeted for sales and services.

In the meantime, the grandmother received another solicitation with the odd name, this time from Rehandart Canada Ltd., which represents those who paint with their mouth and feet. The investigator asked CDMA whether they had any suggestions. CDMA was intrigued by the coupling of the given name and the endearment and offered to follow up with the U.S. Direct Marketing Association. The investigator wrote to Rehandart, which although not a CDMA member, was happy to identify the list broker from which it bought the addresses. The broker identified the list manager who, in turn, identified the source from which the information was drawn—a mail order company selling pantyhose and lingerie.

The list manager offered to remove the name and to determine when the purchase was made and the name entered on the list. He confirmed an order

was made in the incorrect name for a free pair of panty hose, followed by an unpaid order for several pairs. The woman confirmed placing a single order under her correct name (the cheque had cleared) but she returned the solicitation for the larger order under the incorrect name. The company's database included her correct date of birth, telephone number and size, but not the correct name.

Rehandart's list broker found the woman's proper name in the "Lifestyle Selector" list, which is assembled from warranty cards. The trail finally ran dry in the United States where the "Cash Disbursement Centre" (a lottery company) in Laguna Hills, California, did not respond to two CDMA requests for its list source.

It was clear that the information had not come from Canada Post—there was no evidence that it had, and list brokers, managers and the CDMA were unanimous that it did not sell such lists. The Commissioner appreciated the private sector's substantial efforts to help.

Where do they get our names? From us—virtually every subscription, catalogue purchase and warranty registration we complete gets captured in a list somewhere. If you do not want to be on direct marketing lists, say so clearly when you make the purchase. Most reputable companies will respect your request. If you want to get off current lists of CDMA members, write to:

Do not mail-do not call
CDMA
1 Concorde Gate, Suite 607
Don Mills ON M3C 3N6

Harassment investigation notes missing in action
Sometimes the personal animosities that prompt harassment charges spill over into a department's handling of the access requests that inevitably follow.

In one such case an employee filed several complaints that Environment Canada denied her access to records about her performance and qualifications. She had also asked for any documents about the department's handling of a harassment complaint she had filed, as well as those concerning the decision to declare her position "affected" (ie: surplus). The harassment charges stemmed from management's response to her allegations of

irregularities in job classifications, charges the department refused to mediate with the Public Service Commission.

One complaint cited missing witness statements and interview notes gathered by an independent contractor hired to investigate her harassment charges. Also missing were documents from the files of one of two managers she had named in her access request.

The privacy investigator confirmed that most of the hand-written witness statements appeared to be missing from the department's files where they should have been deposited. The contractor insisted that he had given them all to the department, and a witness confirmed having seen them. But only the unsigned typewritten statements could be found. The complainant wanted to see the signed originals rather than the subsequent typed versions.

The investigator also noted that pages appeared to be missing from the information the woman had been given, but with no accompanying explanation. Apparently the contractor had received the incomplete information from one of the managers. The investigator's request for the missing records met a frosty reception from the manager. During a verbal

tussle, he claimed that the information and the accompanying file (which he showed to the investigator but did not allow him to examine) were his personal notes. He threatened to destroy them if the woman sought access. Since he was just a few months away from retirement, he argued he had nothing to lose and there would be no proof that he had done so.

The investigator cautioned him that "personal" or not, the information was a departmental record and covered by the *Privacy Act*. This is often a revelation to government employees. But information public servants gather during their employment for a work-related purpose, is a government—not a personal record. The investigator advised the man to seek legal advice before taking the risky and illegal step of destroying the documents. Although a more senior manager confirmed the investigator's assertion, and staff undertook to get the information, the advice seemed to fall on deaf ears. The investigator was later told that the manager had "lost his file".

This response landed the matter on the assistant deputy minister's (ADM) desk. The manager's office and computer were searched, as was the entire floor in case boxes of his records had been misplaced during a recent move. Although some original records and hand-written notes were found, the investigator could not confirm that it was all the material in the manager's file. The ADM then met the manager to underline his legal obligation to produce the records.

Finally, the man swore an affidavit stating what documents were in his possession at the time of his meeting with the investigator, and that he had not destroyed any documents about the whole affair. Unfortunately this was too little too late; the department should have reviewed the material and disclosed much of it long before in response to the woman's original request.

The investigator then pursued the trail of the signed hand-written witness statements. The contractor insisted he had given them all to the department. When several interviews with staff led nowhere, Office management sought a meeting with the deputy minister. This prompted another search which produced the 20 hand-written statements, as well as the notes the contractor took during his interview with the complainant. The department processed the material and sent it to the complainant almost four years after her first request.

The department was clearly wrong when it maintained it had given the woman all the records to which she was entitled; it had not approached an

obvious source whom the woman named in her request. And the contractor had twice told the investigator he had no further information. Where the records lurked while the investigation was going on has never been established. Given the flawed response to her request, the need for the Office's repeated intervention, and the length of time it took to spring the records, the complainant can be forgiven for her dissatisfaction with the process. Also understandable is her continuing suspicion that other pertinent information exists.

Not surprisingly, the complaint was well-founded.

First spell it out—then get consent

Two complaints illustrate the importance of departments getting a person's clear consent before collecting personal information from or disclosing it to other organizations. Since the consequences for individuals can often be serious, they should be willing participants.

EI disclosure could threaten investigation and future employment
A truck driver registered for employment insurance(EI) with Human Resources Development Canada (HRDC). He noted on the application form that he had quit because the company demanded he work more than the maximum hours allowed by provincial law. He had also filed a detailed complaint with the provincial Ministry of Transport, which agreed to treat his complaint as confidential. MOT advised that they would audit the company.

An employment insurance officer telephoned the applicant to ask for proof of his allegations, along with all correspondence between him and the Ministry of Transport. Then she told him that she would be contacting his former employer.

He explained to the officer at length the problems with contacting his former employer—disclosure could impede the Ministry of Transport audit and risk his being blackballed in the trucking industry. He refused to provide any more information before consulting both his lawyer and his Member of Parliament. She advised that without the information she would disqualify his claim.

Three days later, the EI officer (who has a 14-day deadline to process insurance applications) contacted his former employer. The department

initially denied him employment benefits for quitting "without just cause". The man appealed and a board of referees overturned the decision.

The *Employment Insurance Act* authorizes HRDC to collect information to establish that applicants are entitled to benefits. In the interest of procedural fairness, it must also give both employees and employers an opportunity to give their account of the facts. At the application stage, employers are asked for their version of events and asked to agree with or refute the employees' statements. If decisions are appealed, all interested parties receive all the documentation the board will consider.

Although the truck driver did not tell the EI officer in so many words to stop processing his application, the Privacy Commissioner considered that he had explained forcefully enough to the insurance officer that this was a special situation. She should have suspended the process until she spoke with the Ministry of Transport about its audit, and had clear direction from the driver that he was ready to proceed with his claim—and suffer the possible consequences.

The Commissioner concluded that the complaint was well-founded because the department had failed to adapt its search for facts to the circumstances of the case (as its own policy requires), and disclosed information to his former employer without his consent. The Commissioner was also interested in preventing similar occurrences. The investigator is pursuing changes to HRDC procedures, which would allow EI claimants to withdraw or suspend their applications, and to the EI application form itself to make it clear that by signing, claimants are authorizing contact with the former employer.

HRDC undertook in the short term to issue a bulletin advising staff to ensure clients are aware that former employers are contacted. HRDC is also considering revising its EI brochure and application form to make this clear. As we go to press, neither bulletin nor revisions have appeared.

IRB needs clear consent for criminal checks on refugees A refugee applicant found herself in somewhat similar circumstances after Citizenship and Immigration Canada referred her claim to the Immigration Refugee Board. She completed the required paper work and, after an initial delay, hired a lawyer. A refugee claim officer reviewed her application and recommended a full risk assessment to the presiding board member. Assessments are done to determine what, if any, danger exists for the applicant if returned to the country of origin. The board member rejected

the recommendation because the woman was applying from the United States. It would be unusual for IRB to conduct risk assessments from friendly nations; a criminal records check was considered sufficient.

IRB advised the woman's lawyer that it would conduct the check and asked whether there were any objections. Unfortunately the lawyer withdrew from the case a week after receiving the notice and did not object. Hearing nothing, IRB asked the RCMP to do the records check. The woman did not find out until she retrieved the files from the lawyer two months later. She was very upset and complained that by asking the RCMP to conduct the check, IRB had alerted the U.S. Federal Bureau of Investigations (FBI) to her whereabouts, thus compromising her safety.

The investigator found that the RCMP had responded to the IRB request by checking its own records, not the FBI database. The information appeared in the RCMP database because CIC had asked for a similar check before transferring her case to IRB. At that point, the RCMP had asked for FBI help. The Commissioner concluded that IRB had the right to ask for information from the RCMP and was not the source of the disclosure. The complaint was not well-founded.

However, the decision to proceed with the check without clear authorization from the woman was troubling. Interpreting silence to mean consent to collect more information could be very dangerous for some refugee applicants. The IRB needs to change its procedures to obtain applicants' active consent, and to allow them the option of withdrawing their application before IRB seeks more information. The Office will pursue the matter with IRB.

Disclosing third party's job performance out of line

An employee quit her job at one of Correctional Services Canada's training centres, citing the intolerable working situation. She applied for employment insurance and named another employee who she said would substantiate her description of the working atmosphere.

CSC appealed the decision to grant her employment insurance. In an effort to discredit the other employee before the Board of Referees, CSC gave Human Resources Development Canada several documents criticising *his* absences and work performance, as well as the decision not to renew his contract.

In fact, the man was never called as a witness so his credibility was not relevant. If CSC had needed to challenge his impartiality, it could simply have told the Board that it had not renewed the man's contract. Releasing the details prompting that decision was excessive. In the final analysis, disclosing the man's information may have harmed CSC's case, serving to confirm the tone of the work environment. The Board maintained the decision to grant the woman employment insurance.

The Commissioner considered CSC's disclosure a serious breach of the law. He acknowledged that since the documents had been disclosed, the damage could not be undone. However, CSC apologised to the man and arranged to have HRDC remove and destroy all the documents in its EI appeal files.

Husband's holiday schedule disclosed to verify wife's claim

A Calgary man complained that Canada Post had disclosed his vacation schedule to the Workers Compensation Board (WCB) which was investigating his wife's continuing disability claim.

The wife, also a Canada Post employee, was on extended disability after having been robbed at knifepoint several years before. She had developed several symptoms including acute anxiety, agoraphobia and panic attacks which—despite Canada Post's substantial efforts to modify her job—prevented her returning to work. The woman claimed she could not leave the house except in the company of family or friends.

The extended—and apparently worsening—disability and escalating claim prompted WCB to hire a private investigator to keep the woman under surveillance (including videotaping her activities). As part of its investigation, WCB asked Canada Post to provide the husband's vacation schedule to observe her during family holidays.

Canada Post is obliged to co-operate with provincial WCB investigations and to provide the Board relevant information to administer claims. However, it must also ensure that any information it discloses to WCB—particularly about third parties—is relevant to the request. Although the WCB advised that only it could judge "relevance", Canada Post must also respect the *Privacy Act*. It collected the information to administer vacation credits and work schedules; disclosing it to WCB to investigate another person's claim was an entirely different purpose which the Commissioner did not agree was "relevant". He concluded the complaint was well-founded.

Inquiries

Inquiries virtually levelled off to 10,313 this past year. However, some subjects generated increasing interest, among them were the Social Insurance Number, access to the 1911 census, the Firearms Registry and Bill C-54—the private sector data protection bill. The court's decision on Revenue Canada's disclosure of travellers' customs declarations (see page 84), prompted many calls wanting to know the implications for both individual complainants and the future of the match. The government has appealed the decision.

Calls about the Social Insurance Number almost doubled, prompted perhaps by the Auditor General's critical analysis of its administration, and his observations about its privacy implications (see page 19).

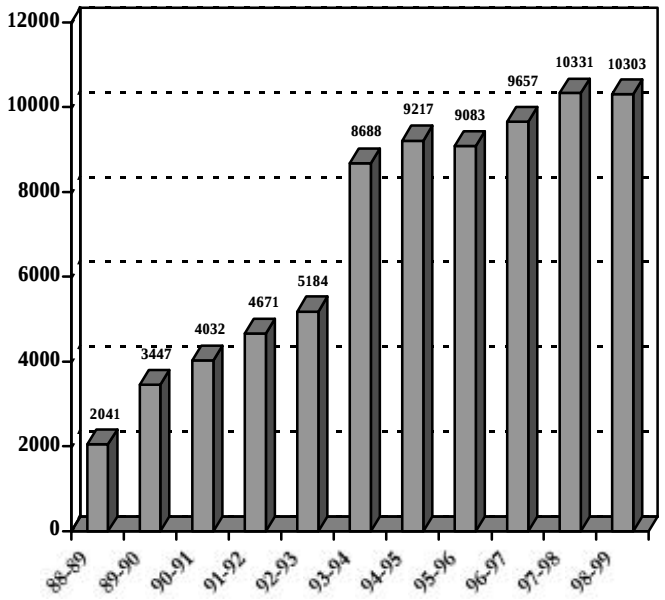
Beginning in December 1998, new purchasers of firearms and many current owners began receiving registration forms for the Firearms Registry. Many callers were worried about the extensive detail being sought, how the information was going to be used, and the security of the information in the registry. The Privacy Commissioner had discussed many of the questions with Senate and House of Commons Committees examining the legislation which created the registry. Neither the legislation or the subsequent regulations spell out the details so many of the questions remain unanswered—an unsatisfactory situation for gun owners and Privacy Commissioner alike.

The following table breaks down the inquiries into broad categories.

Inquiries by Type

Privacy Act, interpretation & process	4399
No jurisdiction, federal	275
No jurisdiction, private sector	503
Redirect to provincial commissioner	885
Redirect to other federal agency	226
Redirect to other	97
Social Insurance Numbers	819
Financial inst., insurance, credit	383
Telecommunications	127
Telemarketing, direct mail	80
Criminal records, pardons, U.S. waivers	142
Medical	79
Adoption, genealogy, missing persons	108
Other	405
Public Affairs (media, publications)	1775
TOTAL	**10303**

Inquiries 1988-99



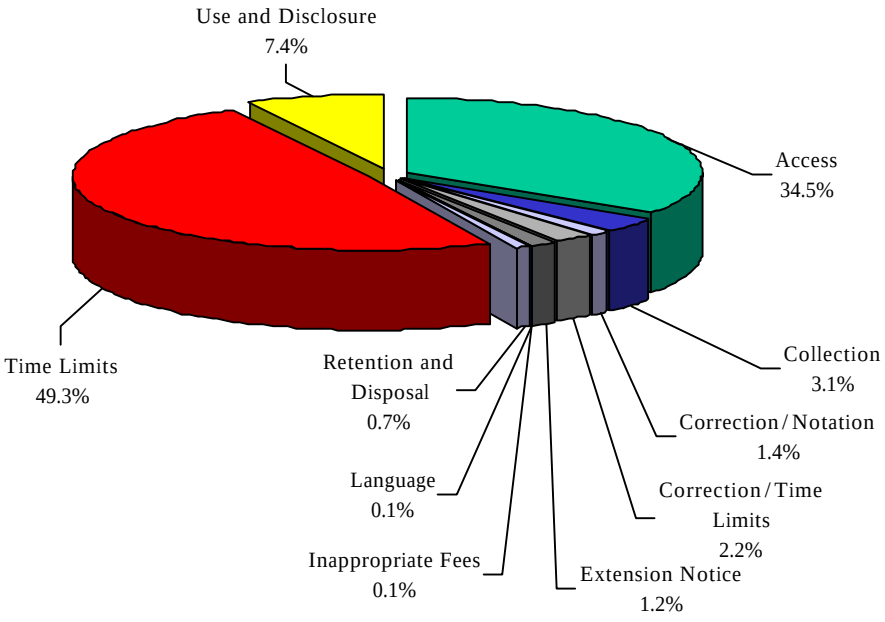
Top Ten Departments by Complaints Received

		Grounds		
Institution	**TOTAL**	**Access**	**Time**	**Privacy**
Human Resources Development Canada	1028	50	65	913
Correctional Service Canada	672	178	455	39
Revenue Canada	665	58	127	480
National Defence	180	50	108	22
Immigration and Refugee Board	121	23	74	24
Royal Canadian Mounted Police	103	73	12	18
Citizenship and Immigration Canada	64	26	33	5
Canadian Security Intelligence Service	48	33	12	3
Canada Post Corporation	29	8	6	15
Justice Canada	28	10	7	11
OTHER	167	80	44	43
TOTAL	**3105**	**589**	**943**	**1573**

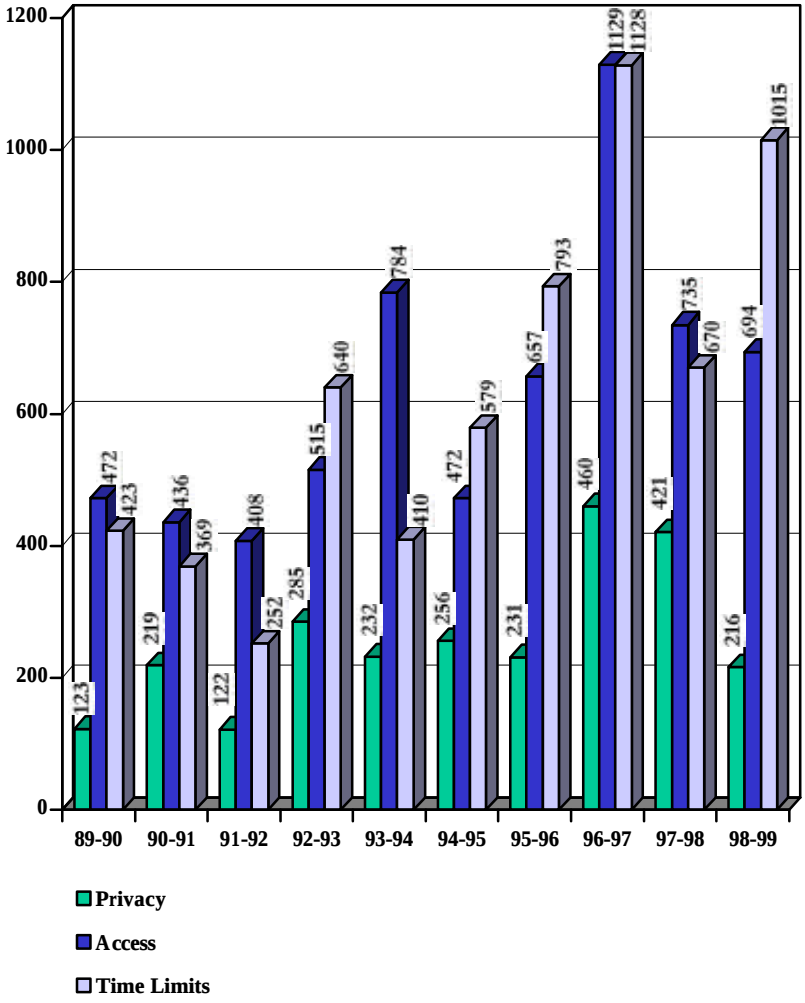
Completed Investigations by Grounds and Results

	Disposition						
Grounds	**Well-founded**	**Well-founded; Resolved**	**Not Well-founded**	**Discon-tinued**	**Resolved**	**Settled**	**Total**
Access	**10**	**86**	**303**	**47**	**30**	**218**	**694**
Access	10	84	293	38	29	211	665
Correction/Notation	0	2	10	9	0	5	26
Inappropriate Fees	0	0	0	0	0	1	1
Index	0	0	0	0	0	0	0
Language	0	0	0	0	1	1	2
Privacy	**43**	**6**	**60**	**27**	**13**	**67**	**216**
Collection	15	0	15	6	4	20	60
Retention & Disposal	1	0	5	1	0	6	13
Use & Disclosure	27	6	40	20	9	41	143
Time Limits	**908**	**3**	**57**	**18**	**0**	**29**	**1015**
Correction/Time	25	0	0	0	0	18	43
Time Limits	873	3	45	17	0	11	949
Extension Notice	10	0	12	1	0	0	23
TOTAL	**961**	**95**	**420**	**92**	**43**	**314**	**1925**

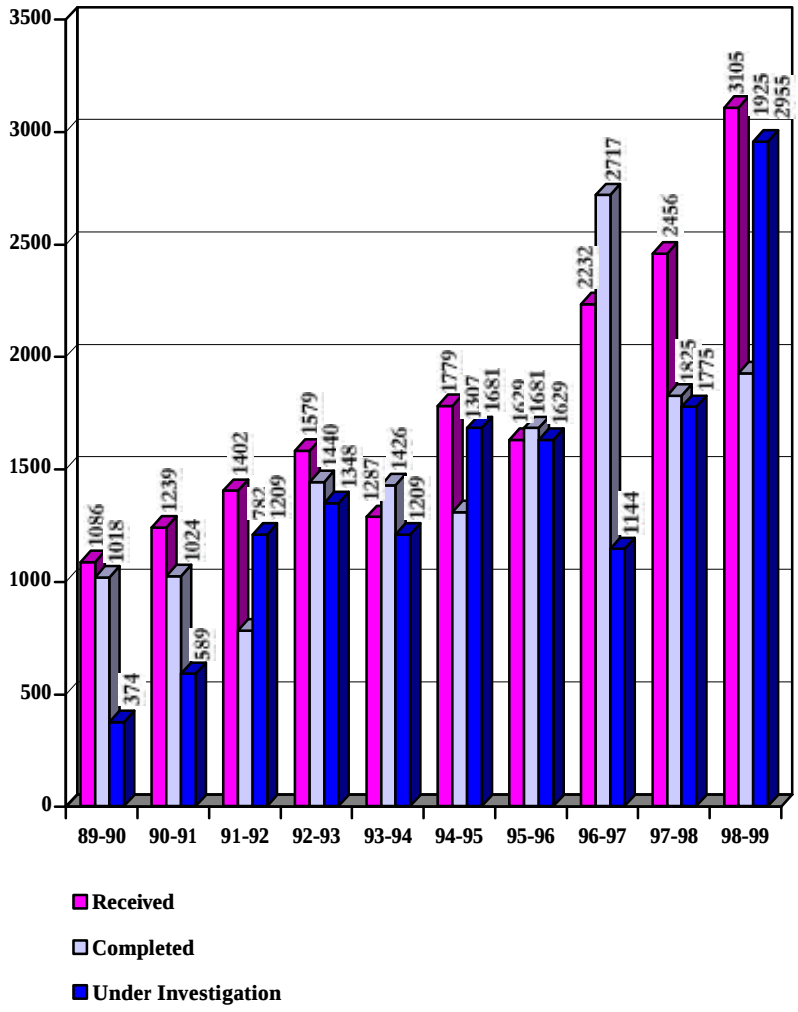
Investigations Completed by Grounds



Completed Investigations and Grounds 1989-1999



Complaints 1989-1999



* The chart reflects minor adjustments to 1996-97 to 1997-98 count

Completed Investigations by Department and Result

Department	Total	Well-founded	Well-founded; Resolved	Not well-founded	Discon-tinued	Resolved	Settled
Agriculture and Agri-Food Canada	3	1	1	0	0	0	1
Atomic Energy Control Board	1	0	0	0	0	0	1
Bank of Canada	1	0	0	0	0	0	1
Canada Mortgage and Housing Corp.	1	0	0	0	0	0	1
Canada Ports Corporation	1	0	0	0	0	0	1
Canada Post Corporation	35	3	2	13	0	3	14
Canadian Heritage, Department of	2	0	0	0	0	0	2
Canadian Human Rights Commission	3	0	1	1	0	0	1
Canadian Security Intelligence Service	48	8	4	19	0	0	17
Citizenship and Immigration Canada	60	16	10	13	3	4	14
Commissioner of Official Languages	1	1	0	0	0	0	0
Correctional Service Canada	679	424	13	147	35	18	42
Environment Canada	24	10	4	10	0	0	0
Farm Credit Corporation Canada	4	1	1	1	1	0	0
Fisheries and Oceans	5	3	0	0	1	0	1
Foreign Affairs and Int. Trade Canada	11	1	1	5	0	0	4
Freshwater Fish Marketing Corp.	1	0	0	1	0	0	0
Health Canada	10	4	1	3	1	0	1
Human Resources Development	141	45	6	13	12	0	65
Immigration and Refugee Board	123	86	5	9	0	0	23

Completed Investigations by Department and Result (cont'd)

Department	Total	Well-founded	Well-founded; Resolved	Not well-founded	Discon-tinued	Resolved	Settled
Indian and Northern Affairs Canada	1	0	0	0	0	0	1
Industry Canada	6	0	1	2	2	1	0
Justice Canada, Department of	45	3	6	20	7	2	7
National Archives of Canada	9	1	0	1	1	0	6
National Defence	246	168	12	28	1	3	34
National Parole Board	19	5	0	6	1	2	5
Natural Resources Canada	6	0	2	2	0	0	2
Office of the Chief Electoral Officer	1	0	0	1	0	0	0
Privy Council Office	9	5	0	3	1	0	0
Public Service Commission of Canada	21	8	2	3	4	1	3
Public Works and Govt. Services	12	6	1	2	0	0	3
RCMP Public Complaints Commission	6	0	0	4	0	1	1
Revenue Canada	241	148	14	46	9	0	24
Royal Canadian Mounted Police	98	5	5	43	10	1	34
Solicitor General Canada	8	0	0	7	0	1	0
Statistics Canada	20	4	1	8	0	6	1
Transport Canada	10	4	2	4	0	0	0
Treasury Board of Canada	2	1	0	1	0	0	0
Veterans Affairs Canada	11	0	0	4	3	0	4
TOTAL	**1925**	**961**	**95**	**420**	**92**	**43**	**314**

Origin of Completed Investigations

Newfoundland	12
Prince Edward Island	3
Nova Scotia	77
New Brunswick	23
Québec	631
National Capital Region - Québec	13
National Capital Region - Ontario	180
Ontario	442
Manitoba	54
Saskatchewan	101
Alberta	78
British Columbia	299
Northwest Territories	0
Yukon	0
Outside Canada	12
TOTAL	**1925**

Update: Privacy Protection in Canada

British Columbia

This year the B.C. Information and Privacy Commissioner developed a series of practical tools to help organizations assess the effects of proposed new technologies or activities on individuals' privacy, and how to mitigate any adverse effects. The documents—*Privacy Impact Assessment, Personal Information Exchange Agreement,* and *Guidelines for Completing an Information Access Research Agreement between a Public Body and a Researcher* are available on the B.C. Commissioner's web site at www.oipcbc.org.

In September 1998 the Commissioner released a report on the collection and disclosure of personal information between health care providers and policing agencies under the BC *Freedom of Information and Protection of Privacy Act.* Following the government's appointment of the Advisory Council on Health Infostructure, the B.C. Commissioner (and other privacy commissioners) addressed the council on the privacy of health information in electronic environments.

Dr. David Flaherty, British Columbia's first information and privacy commissioner, will finish his six-year non-renewable term on July 31, 1999.

Saskatchewan

The provincial legislature passed the first health information privacy law in Canada, May 9, 1999. The *Health Information Protection Act* legislates rights of individuals and obligations of the "trustees" in the health system concerning personal health information (see also page 17).

Manitoba

The Manitoba Ombudsman's Office was designated the independent reviewing agency for access and privacy rights under *The Personal Health Information Act* (PHIA) and *The Freedom of Information and Protection of Privacy Act* (FIPPA). FIPPA has applied to the City of Winnipeg since September 1998, and is expected to be proclaimed for other local public bodies (educational, health care, and local governments) in 1999. PHIA covers persons who collect or maintain personal health information and are health professionals (either regulated by an act of the legislature such as nurses, doctors,

therapists, or designated by regulation); health care facilities (such as hospitals, personal care homes, laboratories); public bodies; health care agencies; and community health centres or other community-based health service designated by regulation.

Although complaint investigation remains a major focus of the Ombudsman's new Access and Privacy Division, its role has broadened to include auditing, monitoring, and ensuring general compliance with the acts.

In March 1999 the provincial government announced public consultations on protecting personal information in the private sector and released a discussion paper. Public meetings were scheduled for April and May 1999. The deadline for written submissions is September 30, 1999. The discussion paper notes that federal Bill C-54, the *Personal Information Protection and Electronic Documents Act* (which will cover the federally regulated private sector) is expected to be passed by Parliament in 1999.

Québec

During the past year, the Commission d'accès à l'information du Québec studied :

1. follow-up by 22 provincial agencies to the Commission's 23 general and 192 specific recommendations made during the previous five years, and
2. security measures taken by provincial agencies to ensure the confidentiality of personal information under their care.

The Commission tabled two reports on the above in the Québec provincial legislature:

- *Un défi de taille: conjuger la protection des renseignements personnels et les pratiques administratives;*
- *La sécurité des renseignements personnels dans l'État québécois au printemps 1998: une démarche bien amorcée.*

The first report concluded that the Commission's recommendations had had very little impact on the workings of the provincial agencies. A follow-up to this report indicated that over half of the recommendations had now resulted in some changes.

The second report resulted from a self-audit by 89 provincial agencies. The results indicated that more than half the agencies provided no training to their staff on the proper method of protecting personal information. The Commission made a number of recommendations and plans a follow-up in the fall of 1999.

The reports are available on the Commission's Internet site at www.cai.gouv.qc.ca.

—and Elsewhere

European Directive in Effect

The European Union data protection directive came into effect in October 1998. The directive obliges member states to ensure that personal information about European citizens is protected when it is exported to, and processed in, countries outside Europe.

Some controversy has arisen over the directive's articles dealing with flow of personal data across international borders. In essence, EU members cannot transfer residents' personal data to a non-member state that does not provide "adequate" protection. Canada is one such country. However, the anticipated passage of Bill C54 should make us one of 40 nations that have adopted or are preparing to adopt laws to protect the privacy and integrity of personal consumer data.

The United States has resisted the tide and developed a set of "Safe Harbor" principles in an attempt to meet the directive's requirements. The principles essentially amount to self-regulation and impose elaborate procedures on consumers wanting to pursue violators. The EU responded last fall to the plan by agreeing not to disrupt data flows to the U.S. while negotiations are under way. As we go to press, the U.S. and EU have failed to reach an accord but negotiations continue.

Study reveals frontline employees uninformed Evidence is mounting about the need for legislation to protect personal information in the private sector, online and off.

A recent study by Ottawa-based Public Interest Advocacy Centre and the Consumer Action Network, based in Montreal, examined the level of

awareness and knowledge of privacy laws and codes by frontline employees of services Canadians use every day: retail stores, financial institutions, transportation companies, and pharmacies. The conclusions are revealing. The researchers found that, despite companies having been subject to privacy codes and laws (in the province of Québec) for several years, customers get different answers about their rights and the company's responsibility for their personal information, depending on whom they ask—and who was asking. The study compared the responses to those given to "mystery shoppers" with those given interviewers who identified themselves, and explained the purpose of the questions. Employees were far less accurate with the unidentified callers, arguably the average customer. No less disturbing is the considerable disparity in staff awareness among the different sectors. Bank employees fared better overall, a finding the study attributed to banks' "significant and ongoing training".

Copies of the 58-page *The Personal Data Protection and Privacy Review* are available from the sponsors.

Privacy Web Seals—Less than meets the eye? A recent outbreak of self-regulatory schemes designed to encourage people to participate in electronic commerce is less about protecting privacy than creating a niche in a lucrative market.

For example, the Canadian Institute of Chartered Accountants has developed CAWebTrust that purports to protect people when they provide information online. The Council of Better Business Bureaus has its BBBOnline seal and, as we reported last year, there is the TRUSTe seal. Others will surely follow.

Using a seal of approval on a web site raises several questions; the most obvious being, how does a member of the public determine which seal is the result of a legitimate assessment of a company's information practices, and which is not? What is to prevent a non-compliant company from simply copying the seal's image from another company's web site and posting it on their own site? This would place a huge burden on someone visiting different Web sites to verify that each site's seal is current, that it has not been revoked and, if revoked, that it had been removed.

There are a several reasons not to rush to embrace self-regulation. The number of on-line privacy violations in the past year is evidence enough. For example, the U.S. Federal Trade Commission investigated several complaints that GeoCities, one of the Web's most popular sites, had turned over

confidential consumer data—including about children—to Web advertisers. The disclosure broke its promise of confidentiality to site visitors and TRUSTe which had granted GeoCities its seal. The FTC reported "this company misled its customers, both children and adults, by not telling the truth about how it was using their personal information".

GeoCities is a member of both TRUSTe and the Online Privacy Alliance, a coalition of business and trade groups that promotes self-regulation as the answer to online privacy concerns. The incident is certainly an embarrassment: as TRUSTe observed "[f]or us, it's our nightmare; this is exactly what we don't want happening". In August, GeoCities agreed to settle FTC charges that it misrepresented the purposes for collecting visitors' personal information. It agreed to post a clear and prominent privacy notice and to seek parents' consent before collecting information from children 12 and under.

Geo Cities is not an isolated example. Consumer fears that they are not well protected on-line are well founded. In the past year, Yahoo Inc., AT&T Corp. and Nissan Motor Co. Ltd. were all reported to be leaving personal data unprotected on their sites, or mistakenly e-mailing personal information to other customers. Microsoft was recently reported to be collecting data on users who had expressly requested anonymity. Even the popular Air Miles Web site left about 50,000 files of Canadian customers unprotected. These examples should serve as a reminder that businesses big and small may not be guarding Canadians' personal data as well as they should.

In the Courts

Robert Lavigne v. The Office of the Commissioner of Official Languages (OCOL)

The Federal Court has ordered the Office of the Commissioner of Official Languages (OCOL) to release to Mr. Lavigne personal information gathered by its staff during its investigation of his official languages complaint.

Mr. Lavigne had complained to OCOL against Human Resources Development Canada. Once the investigation was closed, he asked to see information about him in witness statements and interview notes in the investigation file. OCOL refused him access, arguing that disclosure would "be injurious to its investigation" (s. 22(1)(b) of the *Privacy Act*). Mr. Lavigne complained to the Privacy Commissioner who subsequently intervened in the court action to support Mr. Lavigne's request.

In his October 5, 1998 decision, Mr. Justice Dubé concluded that OCOL did not need to rely on assurances of confidentiality to perform its statutory role as an ombudsman. He also concluded that OCOL had not demonstrated that by disclosing his own personal information to Mr. Lavigne, it would injure this or future investigations. The Court also concluded that the s. 22(1)(b) exemption could not be invoked once the investigation was completed.

OCOL has appealed the decision and the Privacy Commissioner will intervene once again. At press time a hearing date has not been set.

Privacy Commissioner of Canada and the Attorney General of Canada

The Federal Court also supported the Privacy Commissioner's position that Revenue Canada could not legally disclose data from Canada Customs *Travellers Declaration Card* (form E-311) to Human Resources Development Canada to police the employment insurance program.

In her January 29, 1999 decision, Madame Justice Tremblay-Lamer found that Revenue Canada's disclosure of personal information from E-311 forms to the Employment Insurance Commission was not authorised by law. She considered the Revenue Minister's authorisation an invalid exercise of

discretion as it was not related to the purpose of the *Customs Act* and failed to consider the program in question. The government has appealed the decision to the Federal Court of Appeal.

In a second action, the Privacy Commissioner supported an individual complainant's case before an Umpire under the *Employment Insurance Act*. The Commissioner argued that searching every returning traveller on suspicion of defrauding employment insurance violates the protection against "unreasonable search or seizure" as well as the mobility rights of citizens under the Charter of Rights and Freedoms. The case has been heard but the judgment had not been rendered as we went to press.

Corporate Management

The Privacy and Information Commissioners share premises and corporate services while operating independently under their separate statutory authorities. These shared services—finance, personnel, information technology and general administration—are centralized in Corporate Management Branch to avoid duplication of effort and to save money for both government and the programs. The Branch is a frugal operation with a staff of 14 (who perform many different tasks) and a budget representing 14 per cent of total program expenditures.

Resource Information

Although managers continually innovate to deliver services, the Offices' steadily reducing resources have hampered their ability to provide a quality level of service to the public. Treasury Board Ministers noted the impact of this resource and workload crisis at their April 1998 meeting and agreed to a comprehensive (or "A-base") review of the Offices' resource base during the 1998-99 fiscal year. The Board Secretariat is now assessing the report analysis and recommendations and aims to implement the needed adjustments during 1999-2000. The Commissioners anticipate the review's careful assessment of the Offices' resources, service standards and program delivery will resolve the ongoing financial crisis and upgrade its obsolete information systems.

The Offices' combined budget for the 1998-99 fiscal year was $8,128,000. Actual expenditures for 1998-99 were $8,084,150 of which personnel costs of $6,201,525 and professional and special services expenditures of $1,019,179 accounted for more that 89 per cent of all expenditures. The remaining $863,446 covered all other expenditures including postage, telephone, office equipment and supplies.

Expenditure details are reflected in Figure 1 (resources by organization/activity) and Figure 2, (details by object of expenditure).

Figure 1 : 1998-99 Resources by Organization / Activity

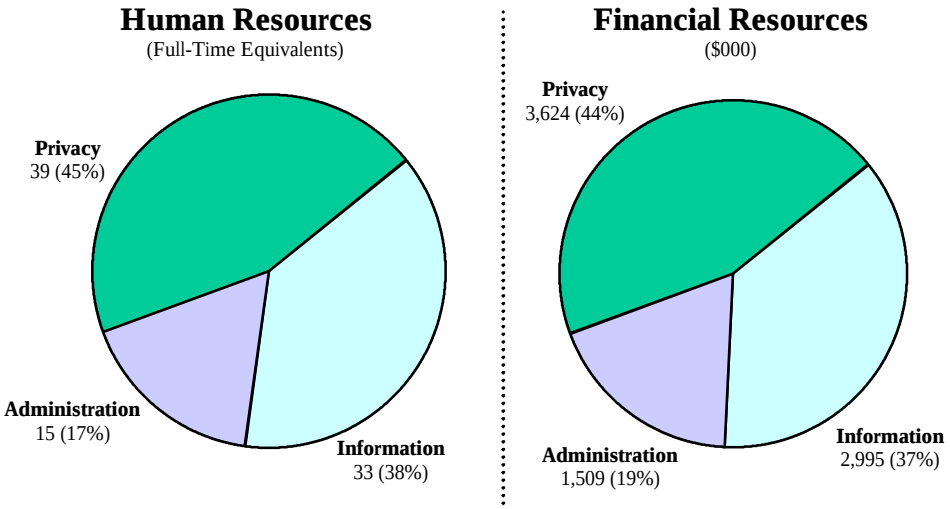
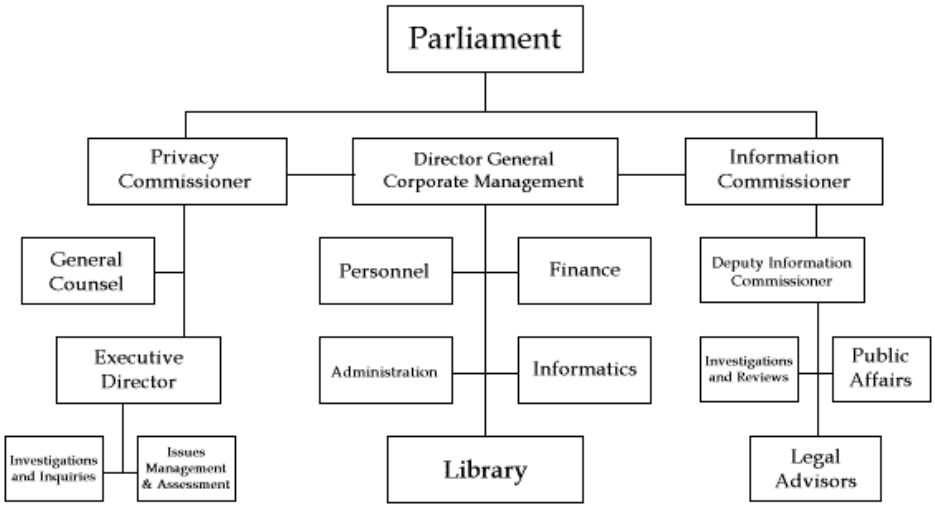


Figure 2 : Details by Object of Expenditure

	Information	Privacy	Corporate	Total
Salaries	2,204,412	2,238,122	705,991	5,148,525
Employee Benefit Plan Contrib.	421,000	491,500	140,500	1,053,000
Transport & Communication	37,351	73,844	105,408	216,603
Information	19,330	43,567	3,907	66,804
Professional & Special Services	207,104	696,583	115,492	1,019,179
Rentals	4,593	5,415	19,402	29,410
Purchased Repair & Maintenance	738	1,995	27,989	30,722
Utilities, Materials & Supplies	24,521	18,428	39,693	82,642
Machinery & Equipment	27,758	58,847	350,287	436,892
Other Payments	224	106	43	373
Total	**2,947,031**	**3,628,407**	**1,508,712**	**8,084,150**

* Expenditure Figures do not incorporate final year-end adjustments reflected in the Offices' 1998-99 Public Accounts.

Organization Chart



A guide to the new private sector data protection bill

Beginning with his 1992-93 annual report the Privacy Commissioner has repeatedly urged governments to recognize that privacy rights should apply to public and private sector alike. Citing the explosion of computer technology, new advances in biotechnology and the blurring lines between the public sector (which has privacy laws) and the private sector (which does not), he encouraged the federal government to provide leadership.

In 1995 Canada's Information Highway Advisory Council called for flexible national privacy legislation based on the Canadian Standards Association (CSA) *Model Code for the Protection of Personal Information*. After public consultation, on October 1, 1998 the federal government introduced the *Personal Information Protection and Electronic Documents Act* (Bill C-54) in Parliament.

Part 1 of this act gives Canadians new legal rights when their personal information is collected, used or disclosed in the course of a commercial activity. The legislation addresses increasing public concerns over personal information practices of the private sector and establishes a new national privacy framework.

Part 1 will also help Canada meet new data protection standards set by the European Union that could otherwise hinder the flow of information to Canada. Quebec is currently the only jurisdiction in North America with a private sector data protection law that meets the EU requirements.

Parts 2 through 5 of the act facilitate the federal government's own use of electronic documents and establish a basis for the legal recognition of electronic documents and signatures. These elements of the act will further stimulate information highway growth and help achieve the government's stated goal of making Canada a world leader in electronic commerce by the year 2000.

When will Part 1 come into effect and to whom will it apply?

Part 1 comes into effect in two stages. Approximately one year after the act is passed, Part 1 will apply to companies subject to federal regulation such as banks, telephone companies, cable companies, broadcasters and

interprovincial transportation companies, with oversight by the federal Privacy Commissioner. It will also apply to a number of federal Crown corporations not currently subject to the federal *Privacy Act*.

In this first stage, Part 1 will also apply to some interprovincial and international data transactions, particularly commercial lease, sale or exchange of customer lists or other personal data.

The second stage begins approximately four years after Part 1 is passed. At that time, Part 1 will also cover all organizations regulated by provincial law unless provincial governments adopt similar legislation. In that case, any organization or activity covered by the provincial law will be exempt from the application of the federal law for activities within the province. The federal law will also apply to all interprovincial and international collections, uses and disclosures of personal information.

The federal government has stated that Quebec will be exempt from the federal law because Quebec's 1994 legislation covers the private sector and is substantially similar to Part 1.

The Privacy Commissioner will work closely with provincial governments and other interested parties to encourage the development of harmonized provincial statutes.

Part 1 contains a primacy clause which will mean that it takes precedence over subsequent acts of Parliament unless those acts specifically provide otherwise.

What types of information will be covered?

Part 1 applies to all personal information about an identifiable individual regardless of form and collected, used or disclosed for any activity subject to the law, with some exclusions. For example, business related information such as name, title, address and telephone number of employees and information used solely for personal or domestic purposes is not subject to the act. Part 1 also excludes information collected, used or disclosed solely for journalistic, artistic or literary purposes.

The CSA Code as a basis for personal information protection

Part 1 requires organizations to comply with the CSA Code (the principles of which are contained in Schedule 1 of the act). The code was developed through a collaborative process by business, consumer groups and government and is considered to be fair, balanced, and to reflect the legitimate interests of both business and consumers. Parliament will review the legislation, including Schedule 1, every five years after Part 1 comes into force.

Individual privacy rights and business obligations

The CSA Code establishes a minimum standard of personal information protection, based on universally recognized data protection principles. The following is an overview of individual privacy rights and business obligations under the CSA Code and Division 1 of Part 1 of the act. Anyone seeking more detailed information should consult the act.

Accountability Organizations are responsible for all personal information within their control and must identify individuals to oversee compliance with the act. This includes implementing policies and procedures, and training employees to protect personal information, as well as informing the public.

Organizations remain responsible when personal data is processed by third parties on their behalf and must use contracts or other means to ensure comparable protection.

Identifying Purposes Organizations must document purposes before they can use any personal information, including the use of previously collected information for a new purpose. Ideally, purposes should be specified to individuals at or before the time information is collected, but must always be specified before use. The purposes must reflect what a reasonable person would consider appropriate under the circumstances.

Consent Except for limited and defined circumstances, knowledge and consent are required for the collection, use, or disclosure of all personal information. Consent may be provided after collection, but, except in certain circumstances, must always be obtained before use. Purposes must be clearly stated and organizations must make a reasonable effort to ensure they are understood. The nature and form of consent must match the sensitivity of the data and the circumstances, as well as the individual's reasonable

expectations. Organizations cannot require consent to the collection, use or disclosure of information beyond that specifically needed for the specified and legitimate purposes.

Individuals can withdraw consent to information use at any time, subject to legal or contractual restrictions and reasonable notice. Organizations must explain any implications of withdrawing consent.

There are some instances where organizations may collect, use or disclose personal information that is subject to Part 1 without knowledge or consent.

Information may be collected without consent if doing so is clearly in the interests of the individual and consent cannot be obtained in a timely way, as well as some defined situations where seeking consent would compromise the availability or accuracy of the information.

Previously collected information can also be used for limited, specific purposes without knowledge and consent. These include investigations into breaches of agreements or violations of laws, life-threatening or similar emergencies, research or study that cannot be accomplished without using the information and where it is impractical to obtain consent, or where the information was collected without consent as described above.

There are similar defined circumstances where information can also be disclosed to third parties without knowledge and consent. These include disclosure to archival institutions and some government institutions. All personal information is subject to disclosure without consent either 100 years after the information was collected or 20 years after the death of the individual who is the subject of the information.

Limiting Collection The amount and type of information collected must be limited to what is necessary for identified purposes. All information must be collected by fair and lawful means.

Limiting Use, Disclosure, and Retention Personal information can only be used or disclosed for purposes for which it was collected, except with the consent of the individual or as required by law. Personal information must be retained only as long as necessary to fulfil the identified or required purposes.

Organizations should develop guidelines and implement procedures for information retention. Information that is no longer required for identified purposes should be destroyed, erased, or made anonymous. Formal guidelines and procedures are required for such information destruction.

Accuracy Personal information used by organizations must be as complete, up-to-date and accurate as necessary for the required purposes, particularly when used to make a decision affecting an individual. Data provided to third parties should also be as accurate and up-to-date as possible, with limits to accuracy clearly specified and understood.

Personal information must not be routinely updated unless purposes specifically require this.

Safeguards All personal information must be protected against loss or theft, as well as unauthorized access, disclosure, copying, use or modification, with safeguards appropriate to the sensitivity. Organizations must take particular care in disposing of data to prevent unauthorized access, and must make employees aware of the need to maintain the confidentiality of all personal information.

Openness Organizations must provide the public with general information on their data protection policies and practices, including the name and title of the person responsible for compliance with Part 1, a general description of the types of personal data held by the organization and its use, and what data is provided to related organizations such as subsidiaries.

This information must be both easy to obtain and understand. Persons with sensory disabilities can request general information or their personal data in alternate formats if the information exists in this format or the cost of conversion is reasonable and the information is needed to exercise their privacy rights.

Individual Access Individuals have a right to examine their personal information and challenge its accuracy and completeness. Organizations must describe what personal information they possess, providing an account of how it is used, and third parties to which it has been disclosed. When it is not possible to list actual parties, a list must be provided of parties to whom the information may have been disclosed. Organizations must amend wrong or incomplete information, with the amended information transmitted to third parties where appropriate. Any dispute over amending a file must be

recorded by the company and details of the disputed data provided to third parties where appropriate.

If asked, organizations must also assist individuals to prepare a written access request. Any data provided to allow an organization to account for personal information use can only be used for this purpose.

Organizations must respond to access requests within 30 days unless there are reasonable grounds to extend the time limit. Individuals must be informed of any extensions and their right to complain to the Commissioner. A failure to respond within set time limits is deemed to be a refusal to respond to the request.

Any costs for personal information access must be directly related to copying costs and be reasonable in the circumstances. A charge may only be levied if an individual is informed in advance of the approximate cost and has agreed to proceed with the request.

When an organization refuses an access request, it must explain the reasons in writing and any recourse. All personal information subject to an access request must be retained as long as necessary for individuals to exhaust all available recourse under Part 1.

Part 1 also identifies a number of limited and specific circumstances where access to personal information can be denied to protect information used in investigations or legal processes, as well as to protect third party privacy rights. Organizations must inform the Commissioner concerning some types of information access refusals.

Challenging Compliance

Organizations must respond to all complaints or enquiries about their personal information handling practices and allow individuals to challenge their compliance with the Code. Every complaint must be investigated and appropriate measures taken to correct deficient policies and practices. Individuals must be informed of any further complaint resolution processes, including their right to contact the Privacy Commissioner.

Filing complaints with the Commissioner

Individuals can file a complaint in writing to the Commissioner when they have failed to achieve a satisfactory response by dealing directly with an organization, or if they believe that a complaint cannot be resolved through such a process. Complaints can be made for any perceived violation of Division 1 of Part 1 of the act, or a requirement or a recommendation of the CSA Code (Schedule 1). There is no time limit for filing complaints, except for complaints about an organization's refusal to grant access to personal information. Access complaints must normally be filed within six months of the refusal. There is no cost for filing complaints.

Complaints investigation

All written complaints will be investigated. In addition, should the Commissioner believe there are reasonable grounds to investigate any other matter relating to personal information protection, he or she can initiate an investigation directly without a complaint. In all cases, the organization will be notified.

The Commissioner has powers to seek and examine any relevant information when conducting an investigation. All information about a complaint investigation is kept confidential by the Commissioner's office. However, the Commissioner may disclose information about an organization's information-handling practices if it is in the public interest to do so.

The Commissioner or a delegate can enter any premises (except a "dwelling place") occupied by an organization, at any reasonable time, examine and obtain copies of any relevant records, and converse in private with any individual on matters relevant to the investigation. There are fines for destroying information that is the subject of a complaint or for obstructing an investigation.

The Commissioner uses dispute resolution mechanisms such as mediation and conciliation in an effort to resolve complaints. These processes generally lead to resolutions much faster, with less expense and with more good will than any other mechanism.

Every investigation must be completed, including a written report, within one year of the complaint being received or the investigation started. This

report is provided to both parties in the investigation, and includes findings and recommendations, the results of any settlement reached by the parties, and any further recourse available to a complainant. The Commissioner can also request that organizations furnish details, within a specified time, of any actions taken to implement report recommendations or reasons why no such actions are proposed.

No investigation report is required in situations where other processes should be used first, where other laws or regulations would provide a more appropriate solution, where a complaint is frivolous or made in bad faith, or where too much time has elapsed between the complaint and its cause. If no report is prepared, the Commissioner will inform both parties and give the reasons.

Applying for review by the Federal Court

The Commissioner has no power to compel organizations to act on the findings or recommendations contained within a report. Within 45 days of receiving a report, either a complainant or the Commissioner can apply to the Federal Court for a hearing on most matters dealt with in Division 1 of Part 1 of the act, including some requirements (but not recommendations) of the CSA Code.

If a complainant applies to the Court, the Commissioner can also apply to appear instead of the complainant (with the complainant's consent), on behalf of the complainant, or as a party to the hearing.

The Court has the power to order an organization to correct its practices to comply with the provisions of Division 1, including notifying the public of any actions proposed or taken to correct practices. The Court can also award damages to the complainant, including damages for any humiliation suffered. There is no limit on the amount of punitive damages that may be awarded. In hearing cases, the Court must take precautions to prevent the disclosure of any information that organizations are authorized not to disclose under Part 1.

Audits

The Commissioner can also conduct audits of organizational practices where there are reasonable grounds to believe that an organization is either violating an obligation under Division 1 or not following a recommendation of the

CSA Code. These recommendations represent best practices that, in some instances, may be a minimum standard of personal information protection depending on the sensitivity of the data, expectations of data subjects, or other factors.

In carrying out the audit, the Commissioner may employ the same powers used in investigating a complaint. As with investigations, it is an offence to destroy personal information that is the subject of an audit or in any other way to obstruct the conduct of an audit.

Once the audit is completed, the Commissioner will provide the organization with a report of the findings and any recommendations. The Commissioner can also publicize the results of any audits in an annual report to Parliament. Although the Commissioner cannot compel organizations to act on audit recommendations, failure to do so could result in a further investigation, leading to an application before the Federal Court.

Education and public consultation

To promote greater awareness of privacy issues and to encourage consistent standards of personal information protection, the Commissioner may carry out public information programs, undertake privacy research, and encourage the private sector to develop and implement policies and codes of practice, based on Division 1 and the CSA Code.

The Commissioner also has a broad mandate to consult with provincial privacy commissioners or other parties, and to enter into agreements to coordinate complaints-handling activities, where appropriate. The Commissioner may enter into agreements with provinces to undertake and publish joint research on privacy issues and to develop model contracts for interprovincial or international protection of personal information. Such contracts can play an important role in achieving consistent standards and meeting international privacy protection requirements.

The Commissioner must report annually to Parliament on all activities relating to Part 1, including the status of provincial privacy legislation and other matters concerning interprovincial and international data protection.

Whistleblower protection

Part 1 protects employers or other individuals from recriminations for acting on reasonable ground and in good faith to uphold provisions of Part 1 or inform the Commissioner of perceived violations. Individuals can request their identity to be kept confidential when contacting the Commissioner. The Commissioner is obligated to maintain this confidentiality in all circumstances.

Employers cannot recriminate in any way against an employee or independent contractor, where they believe an individual, acting on the basis of a reasonable belief, has informed the Commissioner about an actual or potential breach of Part 1, acts directly to prevent a perceived violation, states an intention to do so, or refuses or states an intention to refuse to carry out any duty that would violate the act.