



4th Session, 37th Parliament

REPORT OF PROCEEDINGS
(HANSARD)

SPECIAL COMMITTEE TO REVIEW THE
**FREEDOM OF INFORMATION
AND PROTECTION OF PRIVACY ACT**

Victoria

Monday, July 21, 2003

Issue No. 1

BLAIR LEKSTROM, MLA, CHAIR

ISSN 1708-315X

Published under the authority of the Speaker

In addition to printed transcripts, Hansard Services publishes transcripts
on the Internet and broadcasts Chamber debates on television.

www.leg.bc.ca/cmt

**SPECIAL COMMITTEE TO REVIEW THE
FREEDOM OF INFORMATION AND
PROTECTION OF PRIVACY ACT**

Victoria
Monday, July 21, 2003

Chair: * Blair Lekstrom (Peace River South L)

Deputy Chair: * Mike Hunter (Nanaimo L)

Members: Bill Belsey (North Coast L)
Harry Bloy (Burquitlam L)
* Jeff Bray (Victoria-Beacon Hill L)
* Tom Christensen (Okanagan-Vernon L)
Ken Johnston (Vancouver-Fraserview L)
* Harold Long (Powell River-Sunshine Coast L)
* Sheila Orr (Victoria-Hillside L)
* Barry Penner (Chilliwack-Kent L)
* Gillian Trumper (Alberni-Qualicum L)
* John Wilson (Cariboo North L)
Joy MacPhail (Vancouver-Hastings NDP)

** indicates member present*

Clerk: Craig James

Committee Staff: Josie Schofield (Committee Research Analyst)

Witnesses: Mary Carlson (Office of the Information and Privacy Commissioner)
David Loukidelis (Information and Privacy Commissioner)

CONTENTS

Special Committee to Review the
Freedom of Information and Protection of Privacy Act

Monday, July 21, 2003

	Page
Election of Chair and Deputy Chair	1
Review of Freedom of Information and Protection of Privacy Act	1
D. Loukidelis	
M. Carlson	
Conference Invitation	15
Subcommittee on Agenda and Procedure	16
Other Business	17

MINUTES

SPECIAL COMMITTEE TO REVIEW THE FREEDOM OF INFORMATION AND PROTECTION OF PRIVACY ACT



Monday, July 21, 2003
9 a.m.
Douglas Fir Committee Room
Parliament Buildings, Victoria

Present: Blair Lekstrom, MLA (Convener); Jeff Bray, MLA; Tom Christensen, MLA; Mike Hunter, MLA; Harold Long, MLA; Sheila Orr, MLA; Barry Penner, MLA; Gillian Trumper, MLA; Dr. John Wilson, MLA.

Unavoidably Absent: Bill Belsey, MLA; Ken Johnston, MLA; Joy MacPhail, MLA; Harry Bloy, MLA

1. **Resolved**, that Mr. Blair Lekstrom, MLA be elected Chairman of the Committee.
2. **Resolved**, that Mr. Mike Hunter, MLA be elected Deputy Chairman of the Committee.
3. The Committee received an introductory briefing by David Loukidelis, Information and Privacy Commissioner and Mary Carlson, Director, Policy and Compliance, Office of the Information and Privacy Commissioner.
4. The Chairman and the Information and Privacy Commissioner made note of a conference entitled The State of Accountable Government in a Surveillance Society being held in Victoria on September 25 and 26, 2003.
5. The Clerk Assistant and Clerk of Committees briefly reviewed the work of the committee's predecessor in 1997.
6. A subcommittee on agenda and procedure was struck consisting of the Chairman, Deputy Chairman and Ms. Joy MacPhail, MLA.
7. The Committee adjourned at 10:46 a.m. to the call of the Chairman.

Blair Lekstrom, MLA
Chair

Craig James
Clerk Assistant and
Clerk of Committees

MONDAY, JULY 21, 2003

The committee met at 9:08 a.m.

Election of Chair and Deputy Chair

C. James: If I could have your attention, please. This being the first meeting of the Special Committee to Review the Freedom of Information and Protection of Privacy Act and there not being a Chairperson, I call for nominations for the Chair.

M. Hunter: I would like to nominate the member for Peace River South.

C. James: Any further nominations? Any further nominations? Any further nominations? There being no further nominations, I presume you accept the nomination. If that's the case, I'll put the question.

Motion approved.

[B. Lekstrom in the chair.]

B. Lekstrom (Chair): Thank you very much, and good morning, everybody.

A Voice: That was a close one.

B. Lekstrom (Chair): It was. Very close. It's always nice to see a campaign run so smoothly.

With that, our second item of business this morning is the election of a Deputy Chair. At this time, I'll call for nominations.

J. Bray: I'd like to nominate Mike Hunter.

B. Lekstrom (Chair): Mike Hunter has been nominated. I will call a second time for nominations. I will call a third and final time for nominations. Seeing no further nominations, I will declare nominations closed and ask Mr. Hunter if he would like to accept that nomination.

M. Hunter: I will, Mr. Chair. Thank you.

B. Lekstrom (Chair): Thank you very much. Then we do have a Deputy Chair: Mr. Mike Hunter.

We have been asked to undertake quite a task, which is the review of the Freedom of Information and Protection of Privacy Act. It is a very significant piece of legislation and certainly very interesting. I think most members will have had the opportunity to go through the overview and the introductory briefing that was put out, and I would like to say it was very well done. I think it lays it out very clearly, and we're very fortunate to have that.

[0910]

Today what we're going to do is have a review and a briefing by our freedom-of-information and protection-of-privacy commissioner, Mr. David Loukidelis. As well, joining David is Mary Carlson.

With that, what I would like to do at this time is maybe ask the members of the committee to introduce

themselves. Then we'll turn it over to you, David, and begin the process. I'll start on my right with Mr. Bray.

J. Bray: Jeff Bray, Victoria-Beacon Hill.

T. Christensen: Tom Christensen, Okanagan-Vernon.

B. Penner: Barry Penner, Chilliwack-Kent.

J. Wilson: John Wilson, Cariboo North.

G. Trumper: Gillian Trumper, Alberni-Qualicum.

S. Orr: Sheila Orr, Victoria-Hillside.

H. Long: Harold Long, Powell River-Sunshine Coast.

M. Hunter (Deputy Chair): Mike Hunter, Nanaimo.

J. Schofield: Josie Schofield. I work for the Clerk of Committees office as a researcher for the committee.

B. Lekstrom (Chair): To my left is Craig James, the Clerk Assistant and Clerk of Committees.

With that, just prior to turning the mike over to you, David, I would ask any members of the committee if the agenda.... Is there anything missing or needing to be added at this time?

Things are progressing very smoothly here this morning.

With that, I will turn the mike over. Welcome, and thank you very much for coming out here this morning to begin the process of this review.

Review of Freedom of Information and Protection of Privacy Act

D. Loukidelis: Thank you, Mr. Chair and members of the committee. I hope that as we begin our presentation, the smoothness with which things have gone this morning continues.

I very much appreciate the opportunity to be here with you today. The process on which you're embarking is, as I think the Chair has indicated, one that I think will require of you considerable energy. Certainly, the last occasion on which this legislation was reviewed, beginning in 1998, underscored the dedication and energy that I think will be asked of you. I have every confidence that you'll do your work thoroughly and come up with a report to the Legislative Assembly that will do credit to the legislation and the goals that underpin it.

I'd like to keep things fairly informal today. What we propose to do is that I will begin with some introductory remarks about the legislation and an overview of the policies underpinning both the access-to-information and privacy protection aspects of the Freedom of Information and Protection of Privacy Act.

Then Mary Carlson, who is the director of policy and compliance in our office, will give you an overview of how the legislation works. I will then touch on the whole notion of an independent oversight role, which is, of course, the role that our office plays, and then offer you some unsolicited thoughts on where this process might take you — of course, I offer those, as I say, unsolicited and for the committee to do with as you see fit — and then open it up for any questions members of the committee might have.

I am in your hands, though, Mr. Chair and members of the committee. If there's any thought that you might instead wish to ask questions as we proceed with our remarks, then I think we'd obviously be open to that as well.

B. Lekstrom (Chair): Okay. If the wish of the members is that as we go through it, there's a question that comes to mind.... Certainly raise your hand, and I'll recognize you. We could do it that way. Failing that, we will, at the end of your presentation, go through the question-and-answer then.

D. Loukidelis: The first focus of my introductory remarks is by way of comment on the nature of this process and the role I would see our office playing should the committee wish to take advantage of what I have to say on that point. Section 80 of the Freedom of Information and Protection of Privacy Act, of course, calls on a special committee of the Legislative Assembly to be struck to undertake a comprehensive review, to use the words of the section, of the Freedom of Information and Protection of Privacy Act every four years. It will henceforth be every six years. This is in order to, I think, ensure that the underpinning goals of openness and accountability, on the one hand, and privacy protection as reflected in the language of the statute keep abreast of current trends and meet rising expectations — on the one hand, of the public when it comes to openness and accountability and, on the other hand, the interests of the community as a whole in terms of appropriate protections for government information and personal information — to take two examples.

[0915]

I think it's worth underscoring that this kind of legislative review process undertaken by a committee of the Legislative Assembly is a fairly common feature of access to information statutes around the country. Alberta, for example, has legislation very similar to the B.C. legislation, and a special committee of the Alberta Legislature reported just last year after its comprehensive review of the Alberta legislation. Similarly, the federal access-to-information legislation and privacy legislation was reviewed, for example, by a standing committee of Parliament in the late 1980s and produced this document.

The reason, of course, why legislative committees or committees of Parliament undertake these reviews is that there is a need for, if you will, an arm's-length review of the legislation — arm's length from the execu-

tive branch of government — by the legislative branch of government because of the need to ensure that the analysis of where the balance lies between accountability and government secrecy is appropriately struck.

More immediately, in the context of British Columbia the legislation you'll be reviewing has been reviewed in house, if you will, by government over the last two years, further to a direction given by the Premier to the minister responsible, the Hon. Sandy Santori, on, I believe, June 25, 2001. In April of 2002 and March of 2003 two sets of amendments to the Freedom of Information and Protection of Privacy Act were enacted by the Legislature pursuant to that review. Government has, in effect, over the last two years already conducted its review of this legislation. Of course, the process you're embarking on is of a different character, I would argue. It is a review by the members of the Legislative Assembly, coming to the task, if I might suggest, with a slightly different perspective.

That's not to say that the government's perspective won't be brought to bear. I would expect that although there have been amendments in the last two years, one might argue it's questionable whether government will have anything to say about this legislation as part of your process. I'm quite sure that you will be hearing from the government and that they'll have submissions for you, as will many others, as we'll touch on a little later.

Certainly, we are here today to assure you that in our capacity as an office of the Legislature — because I am, of course, appointed as an officer of the Legislature, as you're aware — we are prepared to do whatever we can to assist the committee. You're in excellent hands, of course, with the staff of the office of the Clerk of Committees in terms of the research support you'll need and other kinds of support. Whatever we can do at any stage during this process to assist you in your work in this comprehensive review we will be prepared to do for you on your request.

Turning to a couple of remarks about the context, if you will, of the B.C. legislation, I think it's important to underscore, as you begin your work, where the British Columbia legislation fits in, not only legislatively within B.C. but in terms of other jurisdictions in Canada and indeed around the world. This coming October 4 is the tenth anniversary of the coming into force of the British Columbia legislation. That really culminated something like 17 or 18 years of work on the part of all political parties on the scene in British Columbia in order to get that kind of legislation enacted.

As you'll see in the briefing paper, back in 1976 the then leader of the Conservative Party tabled legislation, and there followed 17 or 18 years of similar efforts by members of all parties, including the Liberal Party. Gordon Gibson, when leader of the Liberal party, tabled a freedom-of-information act. I think it was in 1977. Other parties, as well, have done so — the NDP party. The Social Credit party, in the last days of the administration in 1991, actually introduced legislation,

Bill 12, but it died on the order paper because of the intervening election.

In 1991 the Mike Harcourt NDP government actually introduced the bill, Bill 50, that became the Freedom of Information and Protection of Privacy Act. There was debate in the Legislature over the legislation, but my recollection is that at the end of the day, the act was passed unanimously by all parties then sitting in the House. I think that underscores the perception that this legislation does not follow the lines of party interest but recognizes the very clear public interest in disseminating as broadly as possible government-held information while at the same time protecting the privacy of individual citizens.

That kind of legislation is now found in over 46 countries around the world, beginning with Sweden in 1766, of all things. As an aside, if I had the time one day, I would love to do the research to find out why it was that the Swedes decided over 200 years ago that they really had to have an access-to-information act.

More recently in the United States, federally, beginning in 1966, the Freedom of Information Act was passed, and other states have followed suit. Now the situation in Canada is that all Canadian jurisdictions — all territories and provinces and the federal government — have access-to-information and privacy protection legislation in the public sector.

[0920]

Turning to the policies underpinning these statutes, the reason they're so widespread and why countries, especially in the former Soviet bloc, have either enacted or are moving quickly to enact access-to-information legislation and privacy protection provisions is, first, on the side of access to information, because of the widespread recognition that openness and accountability are of critical importance to good government in our modern democracies.

Access to information is about enabling and protecting democracy. I really can't improve on the words used by the Supreme Court of Canada in a 1997 decision called *Dagg* against Canada which involved trying to strike the balance between access to information on the one hand and privacy for individual civil servants on the other. As Mr. Justice La Forest said:

"As society has become more complex, governments have developed increasingly elaborate bureaucratic structures to deal with social problems. The more governmental power becomes defused through administrative agencies however, the less traditional forms of political accountability, such as elections and the principle of ministerial responsibility, are able to ensure that citizens retain effective control over those that govern them.

"The overarching purpose of access-to-information legislation, then, is to facilitate democracy. It does so in two related ways. It helps to ensure, first, that citizens have the information required to participate meaningfully in the democratic process and, secondly, that politicians and bureaucrats remain accountable to the citizenry."

Now, I'm sure those are words of great comfort to those of you sitting here today, but I would argue that

they are in fact a recognition of the fundamental importance of this legislation in ensuring that there is openness and accountability in all of our public institutions. As Mary Carlson will indicate, I think, later in her remarks, the British Columbia legislation seeks to ensure that openness and accountability apply across the broad public sector in British Columbia.

In addition to a notion of openness and accountability in democratic processes, I think it's also worth underscoring that access to information is about fairness and accountability in decisions by the bureaucracy. This was touched on in the *Dagg* quote. It's worth remembering that 74 percent, as I recall, of the people who appeal access-to-information decisions through our office are individuals who have, for the most part, been attempting to get at their own personal information in the hands of public bodies. Very, very often they have concrete reasons for doing so. They need their own information in order, for example, to appeal decisions that have been made about their interests by one bureaucracy or another. It's not just about the more sort of diffuse notion of accountability generally in democratic institutions. Access to information is also a tool for individuals to use in order to pursue their own rights and interests.

I think it has to be remembered that access to information, although it is seen as a critical component of open and accountable government, is not by any means a cure-all. I'm not going to sit here today and tell you that access to information is the only way we can keep governments accountable. The point I would leave you with, though, is that access to information is one of an arsenal, if you will, of tools that ensure that our democracies remain vital and that those who are either elected or appointed to positions in society exercise power knowing that citizens have access to an appropriate level of information to allow them to inform themselves to make better decisions at the ballot box and also to have the information to participate meaningfully in debate about policy decisions or specific decisions that are taken in the exercise of statutory powers.

Privacy laws have a slightly different focus. That is, of course, an important part of this legislation. This legislation aims at protecting individual privacy as well. The first point I think you will perhaps find of interest as you begin your work is what it is that we mean by "privacy." What is the concept of privacy that we're driving at in enacting privacy protection laws of the kind we're talking about here today?

Privacy has various manifestations. Back in the 1890s Louis Brandeis, who later became a U.S. Supreme Court Justice, wrote an article in which he argued that privacy is about the right to be left alone. Certainly, there are many ways in which our legal system recognizes privacy in a sense of the right to be left alone. We have laws against unreasonable search and seizure, for example, that limit the ability of law enforcement and security agencies to go into our homes without cause or without warrant. That is a kind of privacy.

In statutes of this kind we are, however, talking about informational privacy, if you will. This is the claim of individuals, as it's been said, to have a degree of control over the collection, use and disclosure of their personal information. It's been called informational self-determination, as Alan Westin, the noted American legal scholar, has called it. The reason we protect privacy in the sense that we protect data privacy is that it is essential not only to individual well-being but to our liberties and, again, to the health of our democracy.

[0925]

I would like to quote from a book called *Big Brother* by Simon Davies, who is a noted international expert, based in the U.K., on privacy and its various issues in the modern age. He says as follows:

"People who have no rights of privacy are vulnerable to limitless intrusions by governments, corporations or anyone else who chooses to interfere in your personal affairs. Imagine a world where government had an unfettered right to demand information from you or to remove money from your bank account or even to enter your house. The tragic history of many of the world's countries shows us that a nation denied the right of privacy is invariably denied all other freedoms and rights."

Data privacy of the kind we're talking about aims at restraining government power and protecting individual liberty, always balanced, however, against the public interests. We need not get into the details today, but you'll very quickly see, as you read part 3 of the Freedom of Information and Protection of Privacy Act, that the privacy rights given to individuals there do not in fact ignore the public interest in the appropriate collection, use or disclosure of our personal information by various government agencies. It is fair to say, however, that the digital age, especially in the post-9/11 world, has increased the risks associated with collection of data by state agencies and the use of that data in ever-evolving ways, especially in light of technological means to mine information, combine data with other sets of data and use them in ways that we might not have foreseen even ten or 20 years ago.

The goal of the B.C. legislation, then, is to impose appropriate restraints, generally called fair information practices, on the ability of public bodies to collect, use and disclose our personal information in order to ensure that we have a reasonable sphere of privacy within which we can continue to flourish as individuals and participate in society.

Now, I'd like to, at that point, turn things over to Mary Carlson, director of policy and compliance in our office, as I said, to give you an oversight of how the legislation works — a few comments on the structure of the legislation and how public bodies across the province go about implementing it.

M. Carlson: I'm going to start off by just talking a bit about the scope of coverage of the B.C. law. British Columbia's Freedom of Information and Protection of Privacy Act probably has the broadest coverage of access and privacy legislation in the country. It covers all

ministries, all Crown corporations, all local public bodies — which include police forces, universities, colleges, municipal governments, regional boards — and it covers all self-governing professions. It essentially covers any public agency that's either fully or partially taxpayer funded. Or, in the case of self-governing professions like the Law Society or the College of Physicians and Surgeons, they perform a significant public-interest role in monitoring those professions, so they're covered as well.

The legislation actually was started in 1993, and it started off by first covering ministries and Crown corporations. The second year it was extended to local public bodies, which are the schools, hospitals, universities and local governments, and then in the third year it covered self-governing professions.

One of the criticisms of the federal Access to Information Act is its lack of inclusiveness and of the large taxpayer-funded agencies that are completely out of the scope, including the Canadian Blood Services, for example, NavCan, Canada Post. Those agencies are not covered by the act, so that citizens have no right to ask for any records in those agencies.

Most of the other jurisdictions have similar coverage. They have patchier pieces. Where their access legislation doesn't cover those public bodies, they have sectoral legislation that covers them.

How do you ask for information? The act applies to records. It's informational privacy, so it has to apply to information that is in a record. A record is anything that stores something in physical form. It could be a photograph, a memo, an e-mail, a voice message. Anything that stores information would be considered a record. We recently had a case where somebody won access to a live webcam feed. A ministry was watching a beehive burner, and the argument was made by Sierra Legal that that was a record. In fact, it's a transient record. It's not being stored on any medium unless the recording camera was clicked on.

[0930]

If somebody wants access to a record, they're required to put their request in writing to the public body they think has the record, and they are required to provide sufficient detail in that request to allow an experienced employee of that public body to be able to locate the record. That's actually a new amendment that happened in April — the addition of requiring people to provide sufficient detail — because a lot of people would put in very broad, vague requests.

People are not required to tell you why they're asking. Their motives are irrelevant in the determination of whether or not they can get access to the record. This is a key point, because prior to this legislation, a person's right to access any record in the custody of a public body depended primarily on the largesse of the person that had the record. If they thought you deserved it or... There were no rules around whether or not records were to be released. When you make a request, you are not required to say why. It's often very helpful just in terms of letting people actually search for the record, but you don't have to provide reasons.

Once a public body receives the request, there's a positive duty in law for them to respond openly, accurately and without delay. They are required to respond within 30 business days. The whole premise behind this is that access delayed is access denied — the idea of getting timely access. It doesn't help somebody who is in some kind of dispute to get access to a record 18 months later. You know, they've made the request, and they need it as soon as possible.

The act requires that within 30 days the public body is obligated to respond to the request and they are obligated to tell the person who's asking if they're entitled to the record and where and how they're going to get access. Typically, public bodies will provide the records at the same time. More importantly, if they are denying access to the record, they are required to give reasons why. That means they have to refer to a specific section in the act that they are using to withhold information.

Public bodies can withhold information. There are 11 exceptions to disclosure. The basic premise of the legislation is that you are entitled to information unless any of the information falls into these exceptions. I'm not going to go into any detail on them other than to point out, for example, solicitor-client privilege. There may be information in a record that, if disclosed, would harm a law enforcement matter, may harm the economic interests of the public body or may invade the privacy of a third party.

In cases where the public body is withholding records, they also have a duty to sever information out of a record. If there is an entire report and there is some information in there that, if it were disclosed, would harm the economic interests of the public body, the public body cannot withhold the entire document. They are required to go line by line and just excise the pieces of information that actually fall under that heading. That's called severing.

Public bodies may charge a fee for accessing records. They are not entitled to charge a fee to anybody who's asking for their own personal information. They're also not allowed to charge a fee for the time they spent severing. They can charge a fee for searching for the records and preparing the records for disclosure and shipping them out. They also can waive the fee if somebody cannot afford to pay or if it's in the public interest. When they're responding, they are required, as well, to advise people that they have a right to appeal the decision to our office. Actually, David is going to go into that at the end.

That is the basic road map of the access part. With respect to protection of privacy, David had referred earlier to some of the rules around privacy. We call them fair information practices. Privacy is not even defined in the legislation. It's defined by a set of behaviours — these fair information practices. Fair information practices are the bedrock of every single piece of meaningful privacy legislation in the world. The EU directives.... All privacy legislation has the same rules. The federal PIPEDA Act has the same rules.

[0935]

What are these rules? Well, they are designed to restrict when you collect personal information, how

you collect it, who you collect it from and how you can use it. Personal information is any information about an identifiable individual.

The first rule concerns collection. Public bodies in this law are not entitled to indiscriminately collect information just because they think it might be useful to have it. There has to be a reason for it. You have to have legislative authority to collect it. It has to be related to a law enforcement matter, or it must be necessary for an operating program. The underlying principle here is necessity and relevance so that public bodies are only requiring citizens to disclose information that's necessary for that transaction.

The idea is to minimize the intrusion in people's lives. There's sort of an exchange theory of privacy. When you're receiving government services, you're required to give out a certain amount of information, depending on the service you want in return. Depending on the service.... If you're going for health care services, you obviously have to disclose some very sensitive information. It runs the whole gamut. We are always encouraging people to minimize what you're collecting. If it's not necessary for the transaction, don't collect it.

One of the other rules is that public bodies, wherever possible, should be collecting information directly from the data subject, from the person whom the information is about. This ensures a certain amount of transparency, because when they collect information, they're required to tell people upfront, "This is what we're collecting, and this is what we're going to use it for," so people understand. If you go into a hospital now, you'll see signs up there saying: "We are collecting your personal health information under the authority of this legislation for the purposes of determining your treatment." And it'll say: "This is how it's going to be used."

There is an obligation on public bodies, when they're collecting personal information, to ensure that the information is as accurate as it can be for the purpose it's being used for, for obvious reasons. Decisions made on citizens about services that are based on inaccurate or incomplete information can have potentially very devastating consequences. It's even more difficult to get that kind of information out of a record once it's in there, so the obligation to keep information accurate is in the law. Citizens have a right to request correction of their personal information if it's inaccurate, and if the public body decides they're not going to make the correction, they're obligated to annotate that record with the correction request.

Probably the most important rules in the privacy legislation are use and disclosure. Once a public body has told a citizen, "This is what we're collecting; this is why we're collecting it," they're obligated to use it only for those purposes. We call it the primary purpose. You can't collect information and then somewhere down the road think: "This is good stuff. We could use all this over here and not tell anybody we're doing that." You'd have to actually go back and get consent from people to do it. This is where our interest in data-matching

schemes always comes into play, because there's a real pull to link databases up and then create a new database of information that was collected for two completely different reasons.

The use is a very, very important part of privacy protection. Similarly, disclosure. There are rules in the act that say when a public body can disclose information, and they can only disclose it in those circumstances. Generally speaking, it's disclosed for the same reason it was collected in the first place.

[0940]

Public bodies are required to maintain copies of personal information they've collected for a minimum of a year if they've used that information in a decision that affected somebody indirectly or directly.

Finally, public bodies are required to take every reasonable step to protect the personal information they've collected against unauthorized use or disclosure or alteration. I can tell you, from ten years in this field, that the biggest privacy disasters that have hit the pages in this province have been because of inadequate security — where you have people running names on databases. There was a case with the Delta police running names of women that were going into the free-standing abortion clinic in Vancouver. We had cases where ICBC files wound up as props on the set of *The X-Files*. All those are investigation reports on our website, but they're very high profile. We cannot stress strongly enough to people that you have to pay attention to security. You just have to do it. All the other privacy protection doesn't really matter if you're not protecting it at the end of the day.

You have a right to complain that your privacy is somehow being invaded by the government if you believe they're improperly collecting your personal information or using it inappropriately. We get a lot of people that come and are objecting to information that's being demanded of them in the first place. There are a whole lot of reasons why people come to us.

David is actually going to talk about what happens when they do come to us.

D. Loukidelis: I mentioned earlier that I am an officer of the Legislature. My job, of course, working with Mary Carlson and others in my office, is to provide independent oversight of compliance with both the access and privacy provisions of the legislation. We have a staff now, including me, of 15 individuals. We have a professional staff of six portfolio officers and a review officer who work under Mary's direction in handling those access-to-information appeals and privacy complaints that come our way.

The access-to-information process works, as Mary indicated earlier, when an individual is disappointed with a public-body decision on an access request — thinks that more information ought to have been disclosed, sought a fee waiver and was denied, believes the public body took too long to respond to the request or has otherwise failed to comply with its duties under the access provisions — and comes to our office and files what's known as a request for review. Really, it's

an appeal to our office to investigate the matter and try to resolve it.

Those professional staff mediate settlements, as we're authorized to do by the legislation, in 91 percent of the access appeals that we get, which is just as well. If we had a lower mediation rate, my ability and the ability of others in my office to write formal appeal decisions would be seriously in question. We get something like 850 access-to-information appeals a year. This last year, for example, we again had more access-to-information appeals than the Ontario information and privacy commissioner's office did. As I say, we mediate settlements in 91 percent of those cases.

In those cases where settlement cannot be reached between the parties through the efforts of one of our portfolio officers or our review officer, the matter then goes to what's known as an inquiry, which is, in effect, a formal appeal hearing. Almost invariably they're done in writing. In four years now in the job I've held two oral inquiries, where I actually convene a hearing in a setting much like this. We have found over the years that it's much more efficient for all involved, including our office — both in terms of costs and, I think, in timeliness — wherever possible to have written inquiries.

What happens is that a notice of written inquiry will be issued by our office. It sets out the issues between the parties that are to be dealt with in the inquiry. The parties will file written submissions, and each will have a right of reply. Typically, public bodies will hire lawyers and will file both affidavit evidence and written legal argument to back up their case. Applicants will similarly make their submissions, almost invariably without a lawyer.

After a period of time, once submissions have been exchanged, when I am able to — I or one of my colleagues, now that I have the ability to delegate the order-making inquiry function — I will issue a written decision. That decision is binding on the parties. It is subject to judicial review in the Supreme Court of British Columbia, and that is something the parties avail themselves of from time to time. Failing any judicial review application and a quashing of the decision, the order is binding.

For example, if I decide that a public body has to disclose the balance of a set of records that it withheld, it must do so. Similarly, if I uphold the public body's decision, if the applicant doesn't appeal to the Supreme Court of British Columbia through a judicial review application, the order stands and the public body continues to withhold the information.

[0945]

On the privacy side the same group of professional staff will have assigned to them by one of our intake officers, who perform the intake function both on the access and privacy side, to look into any privacy complaint that comes into our hands, try to gather the facts from the public body and the complainant and come to a resolution of the dispute.

I think it's a remarkable fact, and it's a tribute to the abilities of the people in my office, that in the ten years

our office has been around, we have yet to issue an order with respect to a privacy complaint. Although we have the authority to order public bodies to stop collecting, using or disclosing personal information — indeed, the authority to order them to destroy information they've improperly collected — we have yet to have to do that. In all of those privacy cases we're able to mediate a resolution of the situation using recommendations. Public bodies have historically had an excellent record of complying with our recommendations that result from the process I've already described. We just issue a letter to them saying: "Here's what we've found, here's what we think went wrong, if anything, and here's what we recommend you do in the future to stop these things from happening again." That has worked very, very well historically.

The other function we play in terms of independent oversight or the other area, I should say, of functions has to do with public education and support to public bodies. We have an explicit mandate to educate the public about the legislation and about their rights and obligations under the legislation. We try to do that as best we can. In recent years the ability to do that has been circumscribed, and we're now at a point where we are finding ourselves essentially performing the more reactive, more passive functions of appeal hearing and complaint investigation.

We do try from time to time, however, to marshal out the resources we have to undertake public education. An example of that is something I'll touch on in a few moments, which is the tenth anniversary conference, which I think you've all been made aware of already. We do try from time to time to hold education sessions for public bodies to ensure that their skills in answering access requests and in dealing with the privacy obligations under the legislation remain current and, indeed, cutting edge.

We have from time to time put on cost-recovery sessions, work sessions or workshop sessions for public bodies around the province in order to ensure that, as I say, they're up to speed on the legislation and that any concerns that arise through staff turnover within public bodies at the local level, for example, are met through ongoing education and training.

The other function we have performed over the years is providing a sounding board, in effect, for government or for other public bodies on the access or privacy implications of proposed legislation, programs or policies. Again, we continue to attempt to perform that role where, for example, ministries might come to us and, having performed a privacy impact assessment, as they're required to do, say to us: "Look, this is a program we're proposing to undertake. We would like your advice on the privacy implications of this proposed program." Again, we do try to provide that service almost invariably through verbal comments, because it's a much more efficient way of doing things. That is something we're prepared to continue to do as best we can in the coming years.

In terms of where we go from here, by way of just drawing our remarks to a close, as I think I mentioned

at the outset, the first review of the legislation began in July of 1998 with a special committee of the Legislative Assembly having been struck for that purpose under what is now section 80 of the legislation. It ended with a report tabled in the House on July 15, 1999, with a series of recommendations for amendments to the legislation, some of which were taken up and formed part of the April 2002 amendments to the legislation to which I referred earlier.

One of the things I think is noteworthy about this kind of process is — and this is an obvious point, I recognize — the need to engage the public in getting the views of the public or particular sectors or bodies involved in what they think about the legislation. The report of the previous special committee that reviewed the legislation lists all of the witnesses who appeared in hearings around the province before the committee.

I think it's remarkable for the breadth of the kinds of groups that were willing to come forward and had things to say about the legislation of varying kinds. For example, you see that the B.C. police chiefs made a submission, the B.C. Library Association, the various regulated professions — College of Physicians and Surgeons, for example, the Law Society of B.C....

[0950]

I suspect you'll have a similarly broad range of groups who are interested in appearing in front of you. I certainly encourage you to take advantage of their expertise, as I'm sure you will. Groups like the Freedom of Information and Privacy Association, as well, and the B.C. Civil Liberties Association, who follow this legislation very closely, as I'm sure you're aware, will have things to say about it one way or another, I'm sure.

I also mentioned that the government may, of course — and it could be expected to, I guess — make a submission. Certainly, we'll be prepared to make a submission to the committee later in your work as you set up the timing and invite those kinds of submissions.

I won't go into any of the issues we're likely to raise at this time. We're likely to have both systemic and specific issues we'll want to raise with you. One issue I'll touch on in passing is a broader issue I've been harping on, I have to say, for about four years now, as have many of my other colleagues around the country, including the information commissioner of Canada, the Hon. John Reid. That's the need for modern information management systems and laws both within the provincial government and also in other governments and public bodies in the country.

I think there is a great fear, as the national archivist of Canada has pointed out, that we're approaching a crisis in information management. The ability of governments to know what information they have, to retrieve it and to make use of it as we pass through a period where we're going to be losing a lot of the managers in the public service, is open to serious criticism — frankly, I think, certainly at the federal level. It's been said by my colleague. I have concerns that this is

something the committee might want to touch upon, at any rate, in order to try to move things forward there.

With that, I'll renew our invitation to members of the committee, Mr. Chair, to attend the conference we're hosting here in Victoria. I know it's at the tail end of the week when the UBCM meeting will be on in Vancouver, but I do encourage as many members as are able to attend the conference on September 25 and 26 here at the convention centre.

It is, as I mentioned earlier, a conference to mark the tenth anniversary of this legislation. We have speakers coming from around the world who are noted experts both on the access-to-information side and the privacy protection side, both from the U.K. and the United States. From the United Kingdom, Simon Davies, for example, will be speaking — and Gus Hosein from the University of London, who is a noted expert on privacy. From the United States we have individuals like Marc Rotenberg from the Electronic Privacy Information Center in Washington, which is really the leading policy think tank in the U.S. on privacy issues. We have representatives from the ACLU.

Closer to home and obviously no less important — I think more important — the Hon. Sandy Santori and the Hon. Geoff Plant will be speaking. We have representatives of the public service here in British Columbia — Ken Dobell is one of our participants, for example — and an array of speakers from around the province and elsewhere in Canada and a keynote speech by the Hon. Lloyd Axworthy as well. Another plug for the specifics of the conference: I think that, primarily under Mary's direction, we've been able to assemble a list of speakers that will — I hope, at any rate, if you're able to attend — give you some really in-depth perspective on a variety of issues surrounding your work, both on the access-to-information and privacy protection sides. I'd be delighted to see all of you there, if possible, and look forward to seeing as many of you as we can.

In closing, with thanks, I think this is, if I may say, an exciting opportunity for this committee to look fundamentally at this legislation and to ensure that it continues on the access-to-information side to deliver on the promise of openness and accountability that is consistent, of course, with the strategic direction set by cabinet in June of 2001. It's certainly consistent with the new-era promise of openness and accountability.

Thank you. I'd be pleased to take questions.

B. Lekstrom (Chair): Well, thank you very much, David and Mary, for the overview. As I indicated earlier, the review document you put forward to the members of the committee, I think, is very thorough and gives a better understanding of most of how this legislation works. As Chair, I think I can speak on behalf of the committee members: we are excited about having the opportunity to look at this, review it and learn a great deal in the process, I'm sure.

With that, we do have members wishing to ask questions. I'll begin with Jeff.

J. Bray: Thank you, Mary and David, for your presentation.

There are just a couple of questions. As you know, I came from the civil service. I lived FOI, like many public bodies do, and I'm a complete supporter of the legislation and its intent. But when Mary, especially, was talking about the fair information practices.... It's sort of the push-me, pull-me section of the act, as far as I'm concerned. You really are balancing sometimes competing interests and sometimes competing theories. I'm just wondering if either of you would like to comment on the current implementation of fair information practices in three different areas.

[0955]

The first is.... I'll use the national child benefit delivery program as an example, whereby people provide information primarily through the Ministry of Human Resources, who administer the B.C. family bonus portion of that program. Now that it is combined with the child tax benefit system federally, there is a requirement for, in essence, two data links to occur. They don't occur in front of people's eyes. They sort of occur up here electronically. It is used in real time to calculate somebody's benefit.

In essence, they gave the province the funds, but it's combined with information that, in a completely different way, they provided the federal government. There has always been a strain, especially on the federal side, as to whether or not we can actually look at their data, and yet the alternative would be, perhaps less efficiently, to provide a benefit to lower-income families in B.C.

There are other examples where — this idea of we've got the information — to share it with another body that's serving the same client means that the same government might be more beneficial, but this firewall is up. I'm wondering if you could comment on something like that, where, in fact, we're having to go back to the client, often a different ministry, to get exactly the same information to provide a benefit they want that otherwise would be less efficient. One of the great criticisms of a lot of government programs is the on-off switch. As soon as a client leaves the program, there's absolutely no idea what's happened with the client. There doesn't seem to be much of a mechanism for follow-up, so the ability to access successive programs is very limited.

The third is statistical studies and whether or not the act is strong enough to ensure that governments can do good statistical studies on various socioeconomic trends or economic trends that protect the privacy of the individual, because it's only statistical roll-ups. From the very specific to the very general, is there a need to look at more of a balance between what's effective and efficient for individual clients dealing with government and the fair practices rules as they currently exist that sometimes mean several branches of government have to go to the same client and acquire the same information?

D. Loukidelis: There is a considerable number of data-linkage or data-sharing arrangements or agreements between provincial government agencies and a

variety of federal government agencies to begin addressing the first question without addressing the specifics of the national child benefit. Those agreements have been in place for some time. My understanding with most of them is that, certainly, the larger concern from a privacy-protection standpoint is generally driven from the federal sphere.

I can give you an example of that. Recent changes to Pharmacare resulted in the need to verify net income levels for individuals claiming benefits under that program, and the privacy protection agenda was very largely driven, quite clearly, by Canada Customs and Revenue Agency's restrictions under the Income Tax Act of Canada when it comes to the disclosure of individuals' tax-related information, hence the need for written consent when you apply for registration with Fair Pharmacare. It was driven by the provisions of the Income Tax Act of Canada as opposed to any restrictions under the provincial legislation.

The disclosure rules about which Mary was speaking earlier are found in section 33 of the Freedom of Information and Protection of Privacy Act provincially. Those were amended in April 2002 to make it clearer that public bodies — certainly, to take the ministerial example, interministry exchanges of information — are able to share information for the purpose of jointly delivering programs or services. That would include benefits, for example. There was a clarification of the legislative language in order to ensure that that could occur.

[1000]

The third point is that you ought always, obviously, to be giving individuals notice that you might be doing that, out of fairness. It provides an element of transparency to citizens. There are plenty of studies from the United States that show you will have a better buy-in from people and will reduce the chances of a complaint about a privacy breach if they know up front that, "Look, we're collecting your information for a specific shared program or service, and we may, in order to more efficiently deliver the benefit to you, share information with other provincial government ministries that are involved in delivering that service or benefit. It's not a question of having always to get consent under part 3 by any means. There are ways of addressing those situations.

Your second point was about the follow-up of clients. It, to my mind, touches on the third point, as well, depending on how you're doing follow-up. Certainly, in the health research area a lot of follow-up on patients in terms of health research, outcomes and so on can be achieved without using identifiable information. It can be achieved by using de-identified data. I'll come back to that in a moment.

If you're trying to follow up on specific clients, again, depending on the details of the program, the kind of follow-up you're trying to do, the ability to share information between agencies that I've already touched on is something that could well be of benefit there. Again, you should be giving notice to individuals that you might be doing that, that you might be

using their personal information to continue to provide them care or services so that they know what it is you are proposing to do.

On the third point, I think the legislation is, in fact, robust when it comes to allowing public bodies to undertake statistical or other research. Section 35 of the act, which has been in place since the legislation was first introduced, I think continues to be a really cutting-edge provision. It allows disclosure of personal information — that is, information about identifiable individuals — for research purposes in certain circumstances. They, I think, are appropriately balanced in terms of individual privacy and the public interest in research, as long as the researcher to whom it's disclosed — and it could be a government agency that is the recipient of the information — de-identifies the information at the earliest possible opportunity.

That doesn't restrict their ability to do the research or analysis. It doesn't restrict their ability, in fact, to do longitudinal research where, over time, they continue to get new data sets about the same individuals. The practice is that they strip the information of the identifiers and assign encrypted new identifiers so that nobody who ultimately has the information in hand knows to whom this data relates.

There is a keeper of the key so that you can continue to dump data sets into the de-identified bin but you are protecting privacy. At the end of the day the researchers don't care. They've got the ability to do their epidemiological or other statistical studies, and they don't, in the first instance, care particularly who those individuals are. Nor are they able to find out, because they don't have access to the key that would link it back.

B. Lekstrom (Chair): Thank you. I'll move to Harold and then Sheila.

H. Long: These are more in the operating area. I just wondered about a few things. First off, you mentioned that written requests had to come in from people for information. Because they're written, those written requests, then, would be available for people that requested them?

M. Carlson: They would, but they probably wouldn't get it. I mean, if I made a request for my own information and somebody then said I would like a copy of Mary Carlson's request for information....

H. Long: You're saying anything that's written that's a document, identifiable — e-mails and so on.

M. Carlson: Right. Conceivably it would become a record as well.

H. Long: Conceivably it's a record, so in fact those records should be made available for someone who is requesting, who possibly has asked for information. They don't have to give out what they're asking for but who has asked for information. That's one question.

The second one is that you made a comment on the record of payment — who pays and how they pay. Do you have a record of who has paid and why they've paid and who hasn't paid and why they haven't paid?

M. Carlson: Well, we don't collect them. You'd have to actually check with CPIA's branch. It would probably have stats on how many fees they've issued. In fact, he has a report out now — we could try and get it to you — that shows how many....

H. Long: No, I'm just wondering if there's a record of payment.

M. Carlson: All we deal with at our end is that when there's a dispute about a fee and it comes to our office, the dispute will either be: "The fee is too high" or "I've asked for it to be waived, and they've refused." Those are typically the circumstances in which our office gets involved, and then we'll mediate those kinds of disputes. With respect to how much has been charged and who is paying, I don't have that information.

H. Long: Should that information be available?

D. Loukidelis: Just so I'm clear, you're saying that....

H. Long: I mean, I put a written request in to find out in the Freedom of Information Act because you made the statement that some pay and some don't pay. How do we know who's paid and who hasn't paid? Whose discretion is this left up to?

[1005]

D. Loukidelis: If an individual makes an access request, let's say, to the city of Victoria, which is one of the public bodies, it will have all of those records. We certainly don't, and we don't have that information. If they charge a fee to that requester and say, "It's going to cost you \$631.21 for access," they'll have a record of whether or not that fee was paid. If you don't pay the fee, you don't get the records. The act says you don't get them.

H. Long: I see.

D. Loukidelis: The public body has quite a hammer there. In fact, the public body can require you to pay a deposit as a condition of even doing any more work on processing the request.

H. Long: But the comment was that some didn't have to pay.

D. Loukidelis: You can request a fee waiver if it's in the public interest or if it's because you can't afford to pay. There's nothing to say the public body has to grant that fee waiver, but their refusal to grant the fee waiver

is something that can be appealed to our office. We do get appeals like that, which again, we mostly settle.

H. Long: There are no hard and fast rules is what you're saying.

D. Loukidelis: The default rule is that the public body can charge fees, as Mary was saying, for certain services and for photocopying and preparing the record and so on. If an applicant doesn't seek a fee waiver, then they either pay the fee or they go home.

M. Carlson: My experience is that if you don't pay the fee, you don't get the record. More people end up paying the fee to get the record than get the fee excused. It's less common.

H. Long: Okay. My last question is: how do you control...? You made that comment on information that is given out for a specific reason. If it's used for another reason, how do you control that? Can you give me an example of a misuse and the consequences of that misuse? How often would this happen? How many times have you either laid a charge or gone after the misuse of information?

D. Loukidelis: We don't have any authority to control use of information; nor do public bodies once it's been disclosed. Certainly, we don't have authority to prosecute anyone. There's no offence under the act for misusing information.

I can give you two examples where they would do so at their peril. These examples would exist even if they didn't get the information through FOI. One is defamation. If somebody misuses information that's been disclosed to them in a way that distorts the information or they misrepresent its content publicly and defame somebody, then they're obviously open to being sued for liable.

A second example is breach of copyright. If somebody gets, through access to information, a copy of a record that somebody owns a copyright in and they then start to use it commercially, they're obviously at risk of being sued for infringement of copyright. All of the civil remedies are still out there for misuse of information, if you will.

M. Carlson: If I can just add there that, typically, what happens is when we're investigating a privacy complaint, all the ministries and Crown corporations have an information and privacy director who is the person we tend to deal with. When we receive complaints — and I can give you two recent examples — from somebody who says, "Someone in that agency has run my name on this database and handed it out, and I think it's this person," we get details from the person who's complained.

Typically, we go back to the information and privacy director, who doesn't know anything about it at this point in time because they've come to us, and we ask them if they could start looking into it from their

end. Nine times out of ten they'll go looking into it. There are audit trails on systems. They'll find out, in fact, that that is what has happened. They step in and take disciplinary action. They deal with it internally. We work with them to review all their systems to make sure their audit trails are proper — what kind of training they've done. We're always seeking some kind of remedial outcome. But very typically, when it's something like that, they catch the person who's done it because of the various trails they leave behind.

H. Long: I think that was my question. My question is — and you were quite emphatic — that the information given was for one use, and they had to state the use. If it was used for another purpose after that, really, there is no way of controlling that.

M. Carlson: Once it's gone.

H. Long: Once it's gone. Emphatic as we want that people are getting information and misusing it, there's not a heck of a lot we're doing about it.

D. Loukidelis: If I could, just one last clause. By contrast, for example, in Saskatchewan's Freedom of Information and Protection of Privacy Act it is an offence to breach someone else's privacy. They have this similar set of rules that we have in part 3 of our legislation.

H. Long: We do not have that in our legislation.

D. Loukidelis: We do not have that in our legislation.

[1010]

S. Orr: A little bit of this has been answered by Harold, but I'm going to move it along a little.

I'm trying to look at the review of this legislation from the voter or the taxpayer on the street, the person we represent — all of us. I'm trying to come at it from that level. I'm going to kind of maybe refer to them as Fred and Alice. Fred and Alice on the street really don't care too much for this legislation and what it reads. They care when they need it, but it's complicated and it's convoluted, and they don't understand it. This is where I'm going to come from. I'm going to come from that person on the street.

I had applied to get some information from my public body. I have gone to the city of Victoria, and I am requesting some information they have. I see the rules. You know, you have severing of certain parts of the document under those 11 exemptions. I understand all of that. Fred and Alice wouldn't understand that, of course, because they wouldn't have had this presentation. They request the information, maybe or maybe not a fee is charged, and they get that information.

I think Harold's point about the piece in the legislation is that once they've got that information, it's game. That stuff is out there. That's not good. There doesn't seem to be any protection under the legislation to stop

that. You just mentioned right now that there was some legislation in Manitoba or Saskatchewan. I can't remember. There was something within the legislation to make that an offence. That piece, I think, is really important — that we need to talk about. Once they receive that information, they can do what they want with it. I just want to throw this out, because I want to get a response from you.

Again, I look at the person on the street. I see that you've got your public bodies that are required by law to take reasonable steps to ensure that personal information... Again, I'd like to know what reasonable steps are being, within this legislation... We are reviewing this legislation to maybe find things in there that we should be putting in. Again, this is more information out there on people that they might not want out there. When I hear your presentation — and I do thank you for it — I see this sort of hole in there that, to me, is the biggest concern for that person on the street — Fred and Alice. If they heard this, they would say: "Well, hang on. How about this information? You know, where's it going?" While we're reviewing this, it's really important that we look at that. That, to me, is quite key.

D. Loukidelis: Just to be clear, the kind of provision I referred to a minute ago in the Saskatchewan legislation really is aimed at the kind of inappropriate access or disclosure by people inside, to which Mary Carlson was referring a minute ago. If I'm understanding you correctly, your concern is: what if an access request is made and somebody gets my personal information, for example? I will not say it's almost impossible for that ever to happen, but it's very, very unlikely.

Section 22 of the legislation provides that in response to an access-to-information request, a public body must not — no discretion — disclose to an applicant information the disclosure of which would unreasonably invade someone else's personal privacy. It then goes on, in a rather detailed manner, to spell out exactly how it is you go about assessing whether or not disclosure would hurt somebody else's privacy.

There are, in fact, a series of presumed unreasonable invasions set out in that section that protect pretty strongly things like medical privacy. Your medical records in the hands of a hospital are technically covered by the act in the sense that somebody could come in and make an access-to-information request to see your personal records from the hospital, but section 22 operates in a way that makes it almost impossible for that ever to happen.

S. Orr: David, in the ten years this act has been in place, have you ever had that happen? Has it ever happened? You would have had their call back. In your records has it happened? How many times?

D. Loukidelis: That somebody has got access to third-party personal information?

S. Orr: Yeah, and have used it.

D. Loukidelis: I don't know about the using part, but it does happen — but when it comes to less sensitive information. A good example is expense accounts of public servants. The way the act works, the information about what they spend is technically their personal information. Theoretically somebody can come in and make an access request for it. I suppose one could argue: "That's my personal privacy. It's none of your business." This is an argument that goes on at the federal level, including recently.

Interjections.

[1015]

S. Orr: I'm sorry, Mr. Chair, but this is really important.

B. Lekstrom (Chair): Go ahead, Sheila.

S. Orr: Thank you. Again, I've got to talk about that person on the street — okay? That person on the street has applied to a public body for information. They get that information, and there's some stuff in there that they maybe could use on somebody else, or they could move that information to somebody. They could hand it over to somebody else. You can't stop that, can you? You can't stop them using that information anywhere.

M. Carlson: If it's been disclosed pursuant to the legislation.... I mean, public bodies say that to us, too, all the time. We have no control over what they're going to do with this information. If it's been disclosed in accordance with the legislation — for example, if I asked for.... Say my brother was killed on the job and I went to the WCB and I asked, as his nearest surviving relative, for that record.

D. Loukidelis: The accident report.

M. Carlson: The accident report. I would get the bulk of the report. Some information might be severed out of it — in the process of interviewing people, people might be disclosing other bits and pieces about themselves, and that might be taken out — but I would be entitled to my brother's personal information in that circumstance. Perhaps the matter goes to appeal, comes to our office, gets resolved, and the report gets disclosed to me. What I do with that is my business after that. We don't control.... Once it's been legally disclosed, there are no controls over it after that. Whatever people try and do with it is up to them.

D. Loukidelis: If I could just add to that to address the second part of your question, the act is well designed to protect third-party personal privacy in that situation. I would contend very strongly that it works very well. There have been difficulties — again, at the federal level — quite frankly, I think, where arguments about individual or personal privacy have tended to get in the way of transparency and accountability. I fully appreciate, though, that there might be concern,

as you say, about the person on the street, who'd be worried about his or her personal information.

Again, the legislation is designed in terms of the substance of the protections for personal privacy — section 22, as I've mentioned — and the decision-making process and the review process through our office. The risks of inappropriate disclosure or use of information are very, very small. I'd ask Mary Carlson to interject if she has different information, but certainly in the four years I've been in the office I can't recall a single complaint coming to us of the kind that you've described.

S. Orr: Well, that's good to hear.

B. Lekstrom (Chair): Right. I'm going to move to our next question, from Tom.

T. Christensen: Thanks, Mr. Chair, and thanks, David and Mary, for the overview. This is sort of bringing back a lot of memories, because when this legislation was first introduced, I was actually fortunate enough to have some involvement through a former life. My recollection from that time was that it was a.... There were a number of very interesting conversations, and it was a great struggle to reach this balance between accountability and protection of information. If anything, we now have a decade of working with the legislation. Hopefully, we've learned a lot in that time. Also, our ability to share information because of technology advances has increased immeasurably.

I want to bring it up to sort of the 60,000-foot level and just.... I recognize that in all likelihood we're going to hear from you both again, but as we go out and are getting presentations from various groups and, perhaps, a number of the public bodies that the legislation covers, can you give us just a really brief overview of what you see as some of the major challenges at this point in time in terms of access to information? At least from what we read in the media, protection of privacy seems to be really where the public's getting really concerned these days.

[1020]

D. Loukidelis: I'll just offer a couple of thoughts before turning it over to Mary if she has any thoughts to add, as I'm sure she will. On the access-to-information side, I think one of the challenges continues to be — and it's another issue that I've been speaking about for a number of years now — ensuring as far as possible the proactive, routine disclosure of records, preferably in electronic form through even web-based public reading rooms, bearing in mind that that only works with general information. You have to be careful about third-party privacy concerns, for example. A lot of records in the hands of the provincial government, certainly, can be got out there more proactively, perhaps, using new technologies.

In 1996 the U.S. Congress passed what are called the EFOIA Amendments, which now set down rules and expectations for U.S. federal government agencies

in terms of providing records without access requests — again, proactively through web-based reading rooms. I think that's an issue and a challenge. It better serves, arguably, in some respects, the interests of openness and accountability that underpin the legislation. It could be more cost-effective, too, perhaps, than relying on a reactive, request-based system as we tend to do now.

On the privacy side, I think that a lot of the challenges actually are driven, post-9/11, by the interests of security. It's difficult in any area, but in particular in this area, to know at this point how you strike the balance between privacy and state interests. A lot of that's been driven by approaches and legislation and programs south of the border, but obviously, it has an impact on us here.

M. Carlson: I would just add to that. In our service plan that we tabled this year we put some high-level points in our annual report of things we see as big issues. One of them is the challenges of alternative modes of governance — outsourcing, P3s — that create different issues around both access and privacy. If you take an agency and you decide that you're going to deliver a service that formerly was delivered by a government agency and was fully covered by access and privacy legislation.... People would have the capacity to make an access request on service delivery choices, for example.

When you shift that and contract that out, that's essentially out of the scope of the legislation. They cover off issues of privacy on a contractual basis, but we no longer have the capacity to investigate if something goes wrong. We can do it.... The intention is that we somehow maintain a role, but the reality is that you can't render a non-public agency — a private company — a public body by contract. It doesn't happen. From our perspective we're always looking to make sure that at least the contracts are as tight as they possibly can be and that there are some real hammers that come down if things go off the rails. That's one of the issues.

As David said, the increase in surveillance in a lot of.... There's a proliferation, for example, of surveillance databases — essentially, databases that are created for no other reason than police surveillance. We had some discussion with Surrey. They wanted to create a methadone surveillance database and make that information available to Surrey bylaw enforcement officers. There's some discussion, for example, of creating databases of people that buy spray paint, to know who may be spray painting — things like that which we're actually doing an investigation into now to make some recommendations. Those are just some ones that are in our recently tabled reports.

T. Christensen: Just on the access-to-information side of it, are there any of the current exceptions in the act that sort of stand out as being used more often than others or, alternatively, that you would like to have a little more scrutiny by this committee?

D. Loukidelis: One that springs to mind, and I alluded to this earlier in passing, is section 13(1) of the legislation, which provides that a public body may refuse to disclose advice or recommendations developed by or for a public body. That provision works, I think, very well to protect the appropriate degree of secrecy or confidentiality that surrounds policy-making functions in any public body.

[1025]

I'm somewhat concerned, in light of a recent court decision on the interpretation of that provision, that it may be time to look at the present language of it and see whether it could more explicitly be directed at the policy-making function, for example, as opposed to a broader range of activities that some have argued wouldn't necessarily have been the intent of that provision in the first place. That's one in particular.

There has been talk out there about the so-called public interest override in section 25 of the legislation. There has been some comment that it's never successfully been invoked by an applicant in the context of a review under the legislation, which is true, although it's a provision that is used. Public bodies use it all the time. Dangerous sex offenders who are being released into the community.... There is a protocol that was developed by what is now the Ministry of Public Safety and Solicitor General, then Attorney General, providing detail as to how you use section 25 to notify the public of these individuals. It is being used, but there are concerns, I know, that have been expressed, both in my decisions and my predecessor's decisions, that, for example, we haven't ever found that that provision actually should trigger disclosure.

B. Lekstrom (Chair): All right. For our next question I will go to Gillian.

G. Trumper: Actually, I think my question has been asked. I'm still sort of processing it. I think I've got the answer. It's very interesting. I didn't know a great deal about it, so I'm certainly going to be at that conference. It's certainly opened my thoughts on it.

I've actually just decided. I've been dealing with a specific one, which I think is FOI, but I'm not sure. That's why I don't really want to go into the question, because I think it might be a bit specific. Maybe I'll ask you afterwards whether or not....

M. Carlson: I don't think you can.

G. Trumper: I'll ask him.

B. Lekstrom (Chair): All right. Are there any other questions of David or Mary at this time?

H. Long: I don't have any questions, but I just want to ask....

B. Lekstrom (Chair): Well, then, please go ahead, Harold.

H. Long: I want your information on whether, in fact, we as a committee should be considering.... Let me just go back on some of the things. I was sort of dog-on-the-bone type thing. On the information. If people or organizations are applying for information — and I mentioned a list — if it is personal, could it not be the person's name and personal? If it's an organization, it could be whoever and what their request is just for that information. There are, lots of times, the possibility that someone's organization could be coming under request, and quite often, you don't know who's requesting and for what reasons. Is there any reason they couldn't have a list like that?

M. Carlson: If I'm understanding your question, I will say that one of the things we do discourage is widespread distribution in a ministry as to who's asking for what information, because there is a sinister element to that. If people are asking for their own personnel records, and the director of personnel, for example, wants to know who in this ministry is asking for their own stuff.... We would actually discourage that from a privacy perspective, because I think it would have a real chilling effect if the fact that I was making a request was widely distributed around.

H. Long: Well, let me give it another take, then. If it's not a personal request — I mean totally personal reasons — could there be a list of people requesting information other than personal?

M. Carlson: I don't think there would be a list. You'd have to go to each ministry. You could probably go to each ministry and ask for the requests. My guess is they'd give you the requests and they'd sever off the actual name of the person who asked.

H. Long: You answered my question. The answer is no.

M. Carlson: The answer is: why don't you ask them and see?

H. Long: I'm going to talk to the committee later. Thank you.

B. Lekstrom (Chair): I'll go back to Tom. He has another question.

T. Christensen: Is there any ability under the legislation to provide third-party consent? For example, could a borrower provide to a lender a consent form that then allows the lender to get personal financial information about that borrower from a public body?

D. Loukidelis: Yes. I mean, to the extent that the request for information about my financial situation.... It's really an access request, but if I've consented to that disclosure as part of my applying for the loan, then there's no difficulty with third-party privacy, because I've consented. You know, it's an informed consent.

That happens quite frequently and is a fairly common occurrence.

[1030]

T. Christensen: Is there any scrutiny of the reasonableness of that request? I guess my concern is that in many private situations where an individual might be asked to provide a consent form, they don't perhaps understand the extent of information they may be consenting to disclosure for. Also, there's often a pretty significant imbalance between the party requesting the consent form and the individual who is being asked to sign.

D. Loukidelis: There's no scrutiny of those issues under this legislation. My understanding is that Bill 38, the Personal Information Protection Act, which is on the order paper for when the House resumes sitting in October, would address those kinds of issues. Consistent with the federal information mentioned earlier, the Personal Information and Protection of Electronic Documents Act legislation, in Alberta and elsewhere, private sector privacy practices will now be subject to some control and scrutiny through the same kinds of fair information practices, with some adaptation to the public sector.

B. Lekstrom (Chair): We have spurred a couple of further questions. I'm going to go to John next.

J. Wilson: I see that municipal law enforcement falls under this jurisdiction. I assume that provincial or federal wouldn't.

D. Loukidelis: The legislation covers municipal police forces — that's right — and other public bodies that have a law enforcement aspect to their activities. For examples, the College of Physicians and Surgeons, it's been held, has a law enforcement mandate in part when it comes to regulating its members, but the RCMP is not, either as the provincial police force or as a contract municipal police force, a public body under this legislation.

J. Wilson: So what type of information would be available to someone who requested it — if, say, they requested personal information — if they were to ask a municipal place for it?

D. Loukidelis: I should add that the RCMP are subject, however, to the federal Access to Information Act and Privacy Act as well, so there is an avenue for access requests and privacy protection through those pieces of federal legislation that do apply. If somebody is asking for information from a municipal police force, there's a range of protections for law enforcement information under section 15 of the B.C. legislation to protect law enforcement activities investigations of municipal police forces.

But if an individual were to come to the police department and say, "I want to see my own file. You were

investigating me last year about a suspected offence. It never went anywhere. You never even recommended to Crown counsel that charges be laid. I want to see what you have on me," that person would be able to make that request and would get parts of the file — again, subject to severing to protect, for example, confidential informants whose identities might be in the file. That would come out, and that kind of thing.

J. Wilson: We've got a system now in the province that integrates all the police units, so any information fed in is now sort of universal, I believe. Would all of that be available through investigation, or is it going to be severed?

D. Loukidelis: I think it's the latter. I think you're referring to PRIME, the acronym — I don't know what it stands for — for the on-line pooling of operational and enforcement information that police agencies are now rolling out across the province. To the extent that that's a record of information, if it resides somewhere in a server, then theoretically an individual could certainly make an application for portions of that record, if you will. In addition to the section 15 protections for law enforcement, which are very, very strong, in my view, you'd have third-party personal privacy issues under section 22, as we've already discussed. Possibly other exceptions would apply as well.

B. Lekstrom (Chair): We'll take one further question, and then.... I know everybody's time frame is quite tight today. We will go to Sheila next.

S. Orr: Very quickly. This actually isn't going to be in the review part of this, but it was something you had mentioned. That was on the public education of the act. How does that...? Again, I've got to back to my Fred and Alice on the street. The public education of this act: how would they know about that?

[1035]

M. Carlson: We do a number of things. We do a lot of public speaking engagements. I must say less so since we've had our budget cuts. It's one of the things that have kind of gone by the wayside. We have a website. We do a lot of public speaking. Groups ask us to come and speak. We have two intake officers that spend 30 percent of their time answering questions from the public. They can just call in and find out how they can make a request or what they need to do. We do our training conferences and our conferences.

That's the extent of it at this point in time.

S. Orr: Thanks.

B. Lekstrom (Chair): All right. Well, that concludes our questions for this morning. I know that as this process goes on, we will be meeting a number of times, I'm sure, to certainly gain further knowledge from yourselves. As that process continues, we will, as well, be going out to the public, as you indicated earlier. We

have a lot of work to do over the next number of months.

Again, David and Mary, I want to thank you for coming and, I think, giving one of the better updates that I've sat in on, certainly. I appreciate your time and effort in this, and we look forward to doing what we have to do as a legislative committee to review this document.

D. Loukidelis: My thanks to the Chair and the committee.

M. Carlson: Thank you.

B. Lekstrom (Chair): Just in closing, on our agenda is the conference invitation. We will certainly make every effort to have as many people attend as we can. I think the more information we can garner as a committee, the better job we'll do in reviewing this legislation.

D. Loukidelis: Again, we look forward to seeing you there.

Conference Invitation

B. Lekstrom (Chair): All right. Our next item of business is for information, really. It is the conference invitation that members have. I know it coincides with other meetings that members have already, I imagine, put on their schedule. I would encourage all members to, if they can't take in the entire conference, take in portions of it, if it's at all possible. As quickly as we can, please review your schedules and get back, as is indicated in the letter, to book into those sessions.

Are there any questions on that?

M. Hunter (Deputy Chair): I do have a question. There's a conference registration fee. Is that waived for members of this committee or MLAs? Do you know? It's a fairly substantial number. That's why I ask.

B. Lekstrom (Chair): I am going to defer that to Craig. I believe it is somewhat deferred. Craig, I would ask your comments.

C. James: There is a reduction in the fee if we register members before, I think, August 1 or something like that.

M. Hunter (Deputy Chair): Thank you.

B. Lekstrom (Chair): Any other discussion on the invitation as it is before us here today?

J. Bray: Would that be a committee expense, though?

C. James: Yeah.

J. Bray: Okay.

B. Lekstrom (Chair): Okay. I will leave that with members and certainly encourage them, if it's at all possible, to take in this conference or a portion thereof. Registering through Craig, definitely, would be appropriate for our committee members.

Subcommittee on Agenda and Procedure

B. Lekstrom (Chair): I'm just going to vary the agenda somewhat before we.... Well, possibly we'll go to item 5 on the agenda, which is election of a subcommittee to deal with agenda and procedure. I put this on here more for discussion. What this really is about is that we have to tour the province and take in some communities — to go out and discuss and allow the public input into this review that's taking place. If it's acceptable to the committee, what I would like to do is possibly have Mr. Hunter and myself put together a schedule versus forming a subcommittee to do this, get it out to the members and ask for your feedback, if that's acceptable.

Some Voices: Aye.

B. Lekstrom (Chair): On this subcommittee would be the Leader of the Opposition as well, Joy MacPhail, who's unable to be with us here today.

If that's acceptable, a show of support.

Some Voices: Aye.

B. Lekstrom (Chair): It's unanimous that we will look after this and get you the information back.

Moving on in our agenda, I'm going to turn the microphone over to Craig just to give a brief overview of what the expectations of our committee are, the time frame set out and the reporting structure that will be put forward to us. We do report to the Legislative Assembly. We are a special committee of that body asked to go out and review this legislation. For further review and update, I'm going to ask Craig to speak on that.

[1040]

C. James: Just for the information of members, we did circulate this morning the terms of reference for this committee. The terms of reference for this committee are identical to the terms of reference for the committee which was struck in 1997. There is reference in the terms of reference to section 80 of the Freedom of Information and Protection of Privacy Act. I'll just quickly read it for those members present.

Section 80 has three subsections: "(1) At least once every 6 years, a special committee of the Legislative Assembly must begin a comprehensive review of this Act and must submit a report respecting this Act to the Legislative Assembly within one year after the date of the appointment of the special committee. (2) A report submitted under subsection (1) may include any recommended amendments to this Act or any other Act. (3) For the purposes of subsection (1), the first 6 year period begins on October 4, 1997."

The reason why this committee was struck just before the House rose in May is because October 4 is a few days before the House resumes sitting in October this year. That's necessarily why the terms of reference were conferred upon this committee.

For the further interest of members, the review which we conducted last time comprised nine public hearings around the province in some of the larger urban centres. Primarily, though, most of the meetings were held in Victoria. A series of briefings were held in Victoria by the freedom-of-information and protection-of-privacy commissioner, along with a government office at the time that was responsible for this matter within government. It's, of course, up to the committee and the members to decide where they may wish to travel to hear the views of the public and others regarding the committee's review.

We have a limited number of copies of the last committee's review of this act, which are available to members. I believe it's on the website. If it's not on the website, we will certainly put it on the website so you can see how the last committee tackled this particular issue. I'll leave it at that. If you have any questions at all about the process the committee followed previously, I'd be very happy to talk to you about them.

The legislation governing the act is on the Internet as well — the website. We can make copies for everybody, if you so wish, or you can print them off at your own station — whatever you wish.

B. Lekstrom (Chair): I know Mike has a question. Then I'll go to Jeff. What we will do as a committee is forward the legislation by e-mail to each member. I would encourage you, probably, to run it off, go through it section by section and begin highlighting any concerns you have or questions on that.

With that I'm going to go to Mike and then Jeff.

M. Hunter (Deputy Chair): When we get the e-mail version of the act, can we be sure it's the consolidated version including the latest amendments?

B. Lekstrom (Chair): Yes.

M. Hunter (Deputy Chair): I wonder: is the service plan of the office of the freedom-of-information commissioner available on the Web?

J. Schofield: Yes.

M. Hunter (Deputy Chair): Can we get the address so I don't have to get lost in...?

B. Lekstrom (Chair): We will forward that at the same time as well.

M. Hunter (Deputy Chair): One last item. The time frame of one year. That's from May — whatever it was — when this committee was given its authority. Is that correct? We have until, basically, the close of the next spring session of the Legislature.

B. Lekstrom (Chair): Yes, we do, and we will do this properly.

The service plan and so on, though, I will point out, is really the purview of the Finance Committee. For us it would be an information issue that we could look at.

M. Hunter (Deputy Chair): That's all I'm asking for.

B. Lekstrom (Chair): Terrific.

T. Christensen: The annual report?

B. Lekstrom (Chair): The annual report as well. We will put together the full information that was presented to the Finance Committee, as well, for the information of the committee members.

I will go to Jeff next.

J. Bray: I was just going to say if we could make sure it's a photocopy of the last report, it would probably be very instructive for us as members.

The other thing is perhaps just informational. Some of us are on several committees. This one will have some travel component to it — certainly the Finance Committee. The Health Committee may also have some travel attached to it, and the Citizens' Assembly special committee may have some travel associated with it. If I might recommend to the Chair and Deputy Chair to at least have some discussion with Craig and the other Chairs. It would be most advantageous to maximize the use of this committee, to not be the third committee to show up in Dawson Creek — that we make sure we are maximizing members' time and we are cognizant of what other committees might be doing.

[1045]

B. Lekstrom (Chair): We will certainly take that into consideration, although I'll point out that Dawson Creek would love to have you again, Jeff.

J. Bray: I'm suggesting that some of us have been to Dawson Creek too many times.

Other Business

B. Lekstrom (Chair): Are there any other questions or other business to be brought before this committee this morning?

J. Bray: Any idea of when we might next convene, or is that what you and Mike will work out at this point?

B. Lekstrom (Chair): Along with Mike we will look to that. I know August is somewhat of a time when many members are going to try and get away for a holiday. I would think it will probably be September before our committee does convene again. The time frame does allow us some flexibility in looking at our travel schedule as well, but we'll be back to the committee members with all of the information we've spoken about here this morning and put together a date and a time for our next meeting. Probably within the next month I'll have that information to you on the date and time for the meeting. Prior to that, though, you will receive all of the information we talked about this morning.

J. Bray: Okay.

B. Lekstrom (Chair): As well, in September we'll probably begin the process of calling for written submissions. We'll put our schedule together, where they can send those submissions and so on. I expect it'll be very well received by the public. There's a lot of interest out there and a lot to learn for our committee. I know I'm certainly looking forward to this and seeing if there's a way to improve on what we already have.

With that, a motion to adjourn has been moved by Mr. Hunter, seconded by Mr. Bray. It is carried. Have a great day.

The committee adjourned at 10:46 a.m.