2010 Legislative Session: Second Session, 39th Parliament
Special Committee to Review
the Freedom of Information and Protection of Privacy Act

REPORT OF PROCEEDINGS
(Hansard Blues)

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

VICTORIA, WEDNESDAY, MARCH 31, 2010

FIPPA - 20100331 AM 002/ebp/0930

WEDNESDAY, MARCH 31, 2010

The committee met at 9:33 a.m.

[R. Cantelon in the chair.]

R. Cantelon (Chair): Good morning, everybody. I'd like to call this meeting of the Special Committee to Review the Freedom of Information and Protection of Privacy Act.

We're very honoured, really, today to have Paul Fraser, the Conflict-of-Interest Commissioner, who is acting as commissioner for the Freedom of Information Act, and with him, some staff. I know that other members will be joining us later, but I'm going to ask Mr. Fraser and his staff to introduce themselves. Then I'll ask the MLAs, starting with Eric, to introduce themselves, and we'll begin.

P. Fraser: Thank you, Mr. Chair. May I introduce my colleagues. On my immediate left is Catherine Tully, the acting executive director of the office. On her left is Helen Morrison, the senior portfolio officer. On my right is Celia Francis, who is the senior adjudicator from the office.

E. Foster: Eric Foster. I'm the MLA from Vernon-Monashee.

S. Cadieux: I'm Stephanie Cadieux, from Surrey-Panorama.

R. Sultan: And I'm Ralph Sultan, the MLA for West Vancouver–Capilano.

M. Dalton: Marc Dalton, Maple Ridge–Mission.

R. Cantelon (Chair): And I'm Ron Cantelon, of Parksville-Qualicum, and your Chair.

D. Routley (Deputy Chair): I'm Doug Routley, Nanaimo–North Cowichan. I'm the critic for Citizens' Services, and I'm the vice-Chair of the committee. I should mention, Mr. Chair, that the majority of our committee are at the House management meeting but will be joining us shortly.

G. Gentner: Guy Gentner. I'm from the very transparent place called North Delta.

R. Cantelon (Chair): Now, in discussing with Mr. Fraser, we're going to proceed through the bulk of the presentation, which will leave probably half the time open for questions. I think, in order to get the context of the presentation framed for us, we're going to allow Mr. Fraser to proceed for approximately 45 minutes, and then we should have lots of time for what, I know, will be many direct questions.

Joining us now are Katrine Conroy and Jenny Kwan, and also walking in is Harry Bloy.

Katrine Conroy and Jenny Kwan. Also walking in is Harry Bloy.

Thank you, Harry, for coming, if not late.

Mr. Fraser, please proceed.

P. Fraser: Thank you. Does this microphone amplify as well as record? It does — okay. And everyone can hear me?

Mr. Chair and members of the committee, I wonder if you can indulge me just for a moment or two. I know that, as Lenny Bruce used to say, nostalgia isn't what it used to be, but I think you'll permit me as people who are familiar with this House to tell you something about what happened 33½ years ago on the topic that we're about to discuss.

Down here I'm holding a copy of the editorial page of the *Daily Colonist*, as it was then known, for Saturday, September 25, 1976. This all falls into the category of you never know what lies ahead and what hat you might ultimately wind up wearing. This editorial — and I won't read all of it — starts as follows:

"The new president of the British Columbia branch of the Canadian Bar Association, Paul Fraser, says he will appoint a committee to draft suggestions to the provincial government for freedom-of-information legislation in the hopes that this province will be the first in Canada to have such a law. What he has in mind is legislation giving persons the statutory right to obtain access to information held by governments or their agencies, with some exceptions, and with any refusal to provide such information or any unreasonable delay or costs subject to review by the courts."

So be careful what you wish for. Here we are all the years later, and of course, you can see how effective I was then. This is 1976. It wasn't until 1993 that the government here was persuaded to bring in the legislation. I did better on the federal scene. It was 1983, as you all know, when the first FOI federal act came into effect. In any event….

All of that you may think I keep in my pillow, but it slipped out of a book quite fortuitously, and I began to think: "Well, there's something cosmic about this committee." It was intended that somehow I should reveal all of this to you. Thank you for indulging me, and Mr. Chairman, I'll make this available for the archives of the committee.

R. Cantelon (Chair): Thank you very much. We'll certainly include it in the minutes, I'm sure. As to cosmic, I don't know. Some of us have been accused of being outerspacely, but we'll see how the day proceeds. We look forward to your presentation.

Harry Lali has joined us. Harry from Nicola.

P. Fraser: Mr. Chair, I want to begin by saying that as we recognize and as the people of British Columbia recognize privacy is both a right and a value. Personal privacy is part of every citizen in British Columbia's DNA. It's as important as free speech, as the presumption of innocence, as the right to equality, as the right to a fair trial. All of that has become kind of trite because of the usage over the years, but it's something that we should not lose sight of in terms of coming to defend and recommend the changes to the legislation which enshrines those principles.

Privacy means different things to different people. To some privacy means the right to be let alone. To others it means anonymity, and to still others it means the right to be unobserved. Under FIPPA privacy means maximizing, wherever possible and to the extent that is reasonable, a citizen's control over the collection, use and disclosure of his or her personal information.

FIPPA is essentially a privacy road map. It contains a set of internationally recognized rules called fair information practices that govern the collection, use and disclosure of your personal information by public bodies.

Collectively, those rules reinforce the basic premise that public bodies must be appropriately restrained, they must be transparent and they must be vigilant in the management of personal information collected in the delivery of public services.

Modern privacy legislation emerged in the late 1960s, when the Council of Europe began studying the effect of computer technology on personal privacy. I mention that because the committee has already heard that FIPPA needs to be modernized, in the opinion of some, to take into account computer technology. But in fact, the very genesis of FIPPA is that it emerged from concerns relating to the effect of computer technology on personal privacy.

You have, I think, received the large submission that's been made by the office, containing as it does something over twenty recommendations. Some of those recommendations are what I'll refer to as housekeeping matters and have to do with changes here and there to the act that would tighten up the process and improve the method of work that we do. Today I am hoping that we can talk in broader terms about the recommendations that address the broader issues that confront us today.

Governments are increasingly turning to sophisticated electronic systems to collect, share, analyze, compile and store often very sensitive personal information of citizens. More and more, our digital selves will be available. That's an interesting concept — our digital selves. Very often, on a lifelong basis, we will see bits and bytes of data about us being accumulated by the government and grow into a kind of construct that may be distorted and only fleetingly resemble our true selves at various times in our lives.

These digital profiles or constructs will very often be used in new ways for administrative and other government purposes unrelated to the original purpose for which the discrete data elements were collected, either to respond to a new policy or legislative directives or in the name of law enforcement or national security.

This concept is known by many as data sharing. By data sharing I mean the programmatic or planned disclosure of personal information by one government agency to another, by one government to another government or by a government to a private sector organization. These disclosures might be one-way, two-way or multifaceted. They may be one-off disclosures or regular planned exchanges of data. Data sharing is likely to occur between or among networked or connecting databases.

Privacy laws, at the moment, give citizens the right to access their personal information and ask for it to be corrected. But in complex data sharing arrangements in complex systems, it's a fair question to ask: "How will citizens even know where their information is or what's been done with it?" Answers to those questions must be found.

The law now says that public servants must collect only that information which is necessary for a given program or activity. Yet given that data sharing is often seen as a critical and legitimate mechanism for protecting, for example, youth at risk, the vulnerable and the sick, will we see a push to liberate our personal data by overturning and relaxing the longstanding principles of necessity and proportionality to achieve these objectives?

One of the things that governments and those interested in the subject of privacy must do is to conduct research — research that would examine real evidence of what's going on out there rather than just accepting bold assertions about privacy barriers. We simply can't allow untested privacy claims to trigger unnecessary and possibly even harmful dilution of the balanced and reasonable privacy rights now found in FIPPA, which is more generous to government in the area of data sharing than any other Canadian privacy laws.

So we come to look at the current environment in British Columbia, having talked about what the future may hold. Currently, there are several empirical examples. I mentioned the necessity to look at real situations, empirical examples from our work at the IPC office, that illustrate the current privacy environment scene in British Columbia.

These examples have to do with, first of all, privacy breach investigations; secondly, e-health investigations; and thirdly, the announced integrated case management system, which featured in the Speech from the Throne in February and about which you've heard submissions.

As a result of the oversight responsibilities which the office has, we receive numerous requests of privacy breaches each year. In response to those reports, we conduct investigations into breaches to establish the causes and to assist in identifying prevention strategies for the public bodies and organizations that are alleged to have been involved.

In the past three years we've investigated, for example, 248 breach reports in both the public and private sector combined. Our most recent investigation report related to the theft of personal information of 1,400 of B.C.'s most vulnerable citizens, about which you've also heard in submissions. Our findings in that case were consistent with many of the breaches that we have investigated in the last three years.

First, government ministries never noticed that the database reports containing the personal information of these 1,400 citizens was even missing. The RCMP had to advise government that they'd found the reports in an employee's possession.

Second, the 26 government employees were aware of the breach, although the majority failed to recognize the situation as a privacy breach, and it took seven months for the government to notify individuals affected by the breach. When notification did occur, the letters were sent to the wrong addresses, resulting in a further inappropriate disclosure of personal information.

We concluded that the results of the investigation illustrated that the government had not yet established what we call a culture of privacy. That isn't, if I may say so, just a buzzword. It's a real expression of concern. We recommended this become a goal of government. In order to achieve that goal, the government must demonstrate that privacy is distinct from, and as important as, other security concerns.

Then, in the area of e-health investigation we've finished and recently published a three-year in-depth investigation of the adequacy of private protections on an e-health system used by the Vancouver Coastal Health Authority. That investigation determined that the software system was designed and implemented with wholly inadequate security. Because of the large number and serious nature of the deficiencies in the security, we were actually unable to publicly report in any detail the nature of those deficiencies — a paradox, I suppose, in this kind of situation.

Personal information was regularly collected, used and disclosed into and out of the system without any authority under the act — under FIPPA. At the time the system was designed and implemented, there were virtually no privacy management frameworks in place. This framework was built over the course of a three-year investigation. It should be noted, with fairness, that there were virtually no privacy management frameworks in place. The framework was built over the course of a three-year investigation.

It should be noted with fairness that the public body was very responsive to our recommendations for improvement, and it made significant progress over the three-year period where the investigation took place. However, this can't change the fact that the system was originally purchased and implemented without a proper privacy evaluation and certainly without adequate security.

All of that to say that in these two examples empirically that I've given you, it could be fairly be said that the material, the electronic material, which is now in hand and resides with either the government or with an agency of the government, is not being managed properly, at least in these two instances now.

So how is that portent for the future? We come, then, to talk about the integrated case management system. As you all know, the system will cost, it's expected, $181 million over the next six years. According to the news release, the system will improve the ability of two ministries — the Children and Family and the Health Services ministries — to share information and to manage individual case files between ministries. So we have the data-sharing situation that I spoke about earlier.

There's no doubt that the system will contain massive amounts of data sharing of personal information about vulnerable British Columbians, including information about welfare eligibility and payments, financial information, information relating to child welfare matters and medical information.

Now, what's important in all of this in part is the extent to which privacy concerns, in this or any system, are contemplated and acted upon, early or at all. The conventional wisdom and, indeed, the reality is that building or baking into software systems privacy concerns is to do it better, do it first, do it cheaper, rather than wait for a system effectively to show that it's inadequate for whatever purposes and have to be retrofitted later on or retrofitted in circumstances where people draw to the attention of the people operating the software that privacy concerns have been ignored.

The planning for this particular system has been underway for two to three years on the basis of all of the information that's been provided by the government in terms of press releases. The government has, after a process, hired Deloitte to become involved, and the government, after a process that spanned somewhere between two and three years, has purchased an off-the-shelf software system, which is now in the process of being implemented. So the system is underway.

I can tell the committee that we have requested, the office has requested, over the last two and more years a privacy impact assessment from the government, and one has yet to be received. It is an essential tool in ensuring that a system or a project will be compliant with the privacy requirements of FIPPA, and that particular section of FIPPA which provides for a privacy impact assessment is one that has not often enough, in everything that I've been able to see, been accessed, implemented and taken advantage of by governments or other public institutions.

The reality is that in a system like this the privacy impact assessment, which is so necessary, is not likely to occur, now with certainty, until after the installations or the development of the system is underway.

The act, FIPPA, requires that there shall be such a privacy assessment. The act is silent about when that assessment must be filed. One of our recommendations is to tighten that up and provide a temporal timeline for that, but the act requires that the assessment must be filed.

Now, stepping back from that and speaking calmly, I think that most British Columbians concerned, for example, about their environment would be astonished if environmental assessments, which are regularly done around the province, weren't performed on any project where there was potentially an environmental impact. We all know that there are a variety of legislative provisions that guarantee that that will be so.

Here is a provision in FIPPA which, if it hasn't been ignored, certainly hasn't been complied with — a difficult situation, in my respectful opinion. The section of FIPPA, for your note taking, that I've referred to is section 69.

The example that I've just given you — the examples of the e-health and the example with respect to the 1,400 patients — illustrate that in our experience public bodies in British Columbia have not learned how to build privacy into their projects.

Understandably, they have service delivery goals that they wish to meet. Unfortunately, expediency has consistently trumped privacy, and it puts the privacy of British Columbians at some, I'm bound to say, significant risk.

With respect to FIPPA, it is what I suppose could be referred to as core legislation, consistent with every other jurisdiction in Canada in terms of both its structure and its rules. It's based on internationally recognized principles, as I mentioned, and any substantial change — such as those that are recommended by the government, with respect to the integrated case management system — should be viewed with great care and only undertaken after detailed evaluation of unanticipated consequences.

In saying that, I say it once that I don't dispute for a moment the legitimacy of the effort that the government is making to try to share information across the government for all kinds of reasons. What I do say is that we can't be at risk of throwing the baby out with the bathwater, if you'll let me say that, and abandon, somehow in the name of expediency and good management, the privacy concerns that are at the centre of all that we do in terms of protecting that privacy as citizens in this province.

Our submissions, in the written document that we filed, anticipated that information sharing for integrated service delivery would be a key element of the government submission, so we haven't been taken by surprise.

The government submission was just discovered by our office, on your website, on Monday morning of this week, so I'm not able to give you a detailed, bulleted, point-by-point answer to some of the concerns. I hope that to the extent that those concerns will develop and could be particularized and maybe helpful to you in your work that we'll be able to deliver those to you after the fact.

Where the government's position seeks to fundamentally change the rules that exist in FIPPA to address the concerns that arise from the case management system, our submissions address these same concerns while maintaining FIPPA's essential integrity.

We recognize the public value in integrated service delivery and information sharing in appropriate circumstances, and I can assure you that we have provided recommendations that allow government to take advantage of modern technology while still protecting privacy as a fundamental value.

The point of the work that we have done in this area has not been to simply complain or flag discrepancies and deficiencies but also to try to make suggestions which a committee like this is able to consider in the public interest.

Our view is that there is no need toadd or amend any of the privacy rules in FIPPA, that they are already sufficiently broad and flexible enough to accommodate integrated service delivery.

In the oral submissions the government representatives repeatedly noted that public bodies are confused about the meaning of certain provisions of FIPPA and take different approaches to interpretations of the same section. We agree that the fundamental issue is a lack of understanding that public servants have with respect to some of the provisions of FIPPA. But the answer, in our respectful opinion, doesn't lie in creating a new set of rules, but rather in providing leadership and clarity around the existing rules.

Some of the questions that were put by members of this committee to the government representatives had to do with apparent — I'm going to say apparent, not real — deficiencies in FIPPA. Some of the examples were tragic, and you'll be pleased, I hope, to know that we are going to deal with all of those examples in the course of the submissions — and probably the answers to other questions you may have — to show you that the document, or at least the legislation, is organic legislation, if I can use that term. It's legislation that has been like a moving platform. It's been adjusting for years and years and years to technological change.

That's made the legislation, without question, complicated. It's made the legislation not easy, at first impression, to interpret and to understand. But the legislation is, I can assure you, in a form and shape at the moment where all of the circumstances that were being contemplated by the government as being necessary to eradicate in order to make sure that the case management system could survive and prosper are already catered to in FIPPA.

So what key privacy recommendations have we made in respect of the empirical work that we've already done and are coming to make in respect of the case management system and other things, coming forward?

The first thing that we've recommended is that there be a code of privacy practice, which would be of assistance to those people who actually have to, on the ground, be the RCMP person in the cruiser car, actually have to be the person knocking on the door trying to deal with a potentially tragic situation. How can they, in fact, understand what they are or they are not entitled to do? Because that seems to be one of the concerns, and it's a legitimate concern.

If the act is unintelligible then we've got to do something about that. I'm saying that the act is complicated — there's no question about that. But it's the training, the learning and the guidance with respect to the act that, frankly, has been missing.

One of the ways, in our view and with respect to recommendations that we've already made, that could be accomplished is to have an appointment made of what we call a chief privacy officer for the province. That was the centrepiece of the recommendations that we made in respect of two of the reports that I've referred to earlier. The idea was that that person would be, if you like, the bright line that people who had line responsibility could follow, where they could get the information out about what the privacy concerns really were and what they had to do with respect to sharing information.

That's a recommendation which we have made and I make again today as strongly as I am permitted, Mr. Chair, to make it.

That privacy officer would have to be at a level of executive authority where the person could, in fact, give direction and be available as a resource across the government to all ministries that were looking to have their members properly instructed and informed about the interpretations of FIPPA under circumstances that are likely to develop.

We have recommended that — and it's in the larger document that we file — with respect to the case management system and with respect to the whole issue of data sharing, which is here and which is going to be here for the rest of our lifetimes in its present and even more refined circumstances, that there be a process of public consultation so that those who see their privacy at risk will at least be able to engage in an effort which, therapeutically if nothing else, will show how that privacy is indeed going to be protected or not. Out of that, some good must inevitably come.

My predecessor recommended in his annual report of, I think, a year ago, that there be a kind of white paper process where there would be the government announcing its intention and people would be able to make submissions. That process is well known in the United Kingdom, has been tried in federal government in Canada and I don't think has been tried in British Columbia.

There's something, if you don't mind the colour references, also called a green paper, which, those of you from political science 101 will remember, is what used to happen in the United Kingdom when the government didn't have an actual policy, but it had some ideas and it wanted the population to respond to them. Green papers were an active and successful form of communication, and there may be some purpose here for that sort of thing.

If you're going to deal with the privacy of individuals in digital form, and if there is a concern, as it would appear there clearly is, then the worst thing to do is to seek to impose something. The best thing to do is to discuss how whatever you're going to do is going to work, and how it might be improved.

One of the other aspects of privacy and regulation, or some may say over-regulation, is voluntary disclosures. The committee has already had some questions and answers with respect to that kind of a system in your session with the provincial government representatives. It's a fact, of course, that the process of demanding information is a process that could be mightily assisted if the information were to simply be provided on the basis that there is a right to know what the government is doing in all of its various manifestations. And if the information is put out and people receive it, that's got to have, inevitably and logically, one would think, some effect on the back end of the process in terms of how many demands there would be for information.

It's interesting in this context. Of course, comparisons sometimes are or they aren't relevant, but on the 21st of January, 2010, shortly after he was inaugurated, President Obama issued two executive orders. We have copies of this, Mr. Chair, if the members are interested in seeing it, which we can leave with you. The first one had to do with the Freedom of Information Act, legislation that has been federally in place since roughly 1966 in the United States.

In this directive, the President says: "In our democracy, the Freedom of Information Act, which encourages accountability through transparency, is the most prominent expression of a profound national commitment to ensuring an open government." Later: "All agencies should adopt a presumption in favour of disclosure in order to renew their commitment to the principles involved in the Freedom of Information Act, and to usher in a new era of open government. The presumption of disclosure should be applied to all decisions involving the act."

"The presumption of disclosure also means that agencies should take affirmative steps to make information public. They should not wait for specific requests from the public. All agencies should use modern technology to inform citizens about what is known and done by their government. Disclosure should be timely."

That has led to, as we know, various reading rooms that have been set up across the United States where citizens can go in on the computer, instantly get information from their government, which until this directive came into effect — at least not to the same extent — might not be on the screen. So people would be able to get all kinds of things simply by accessing the government web.

In addition to that, the President on the same date issued an order with respect to transparency in open government. The effective words were:

"My administration will take appropriate action, consistent with law and policy, to disclose information rapidly in forms that the public can readily find and use. Executive departments and agencies should harness new technologies to put information about their operations and decisions online and readily available to the public."

So if there is some question that we are in a time warp here and that FIPPA is some kind of sea anchor and some kind of ARDVAC in a system that should be swept away today in order to introduce some modernization, you can see that as recently as four months ago, at least the United States is having a reaffirmation of the value of the act and, perhaps equally important, a renewal of a determination to get on with voluntary disclosure of information. That's a development that can only be applauded.

In the recommendations that we have filed with you, we have also addressed a separate item which is called the duty to document prescribed government decisions. A right to access can only be exercised if a record exists, and in the past

three years the office has investigated over 1,100 complaints that public bodies have failed to respond openly, accurately and completely to access requests.

The main source of these complaints is the belief that a document should exist, but hasn't been produced has resulted in the complaint. We have recommended, therefore, that there be a creation of a duty to document. We don't propose that this be an onerous duty, but the proposal suggests that some duty should be imposed on public servants to record actions and decisions and reasons therefor. It seems to me, with respect, a fairly low threshold.

Now, Mr. Chair, I wanted to respond to some of the government's oral submissions in an attempt to deal with the various incidents and matters that I referred to that we would deal with in the course of what we have to say.

The government's position, as we understand it, is that FIPPA needs to be modernized, that horizontal government and integrated service delivery is to be preferred to the kind of vertical delivery and silo efforts that currently take place. They talk about principle-based rather than rule-based prescriptive rules as an approach. They say that FIPPA is too complicated, and they talk about the phenomenon of collection by consent.

One of the solutions that is seen to the problems that have been identified by the government is to add consent as an authority for collection of personal information.

As I mentioned earlier, in terms of FIPPA itself, it's not correct — with respect — to say that FIPPA was drafted without taking into account the implications of modern technology. It was drafted because of those implications. We agree that FIPPA should be continually modernized to reflect changes in information technology in government practices. Our submissions provide recommendations for changes to both access and privacy provisions that take advantage of modern technology but maintain the fundamental provisions of FIPPA.

The government submission, in my submission, would profoundly alter the essential foundation of privacy protection in British Columbia. The proposed changes in total would so fundamentally loosen the rules regarding collection, use and disclosure of personal information that privacy protection would in effect, or could in effect, be at the discretion of public servants. And I don't say that in a pejorative way about public servants. What I say is that people are having, under the system that, as I understand it, is being proposed, to make decisions in circumstances where there is already legislation that is there to help them.

Government provided examples of how FIPPA interfered with government projects. Based on our review of the transcript of what was said in the presentation and an initial review of the submission, briefly, we were unable to identify exactly how the government had determined that FIPPA interfered with these projects. All of the examples are either permitted or are permitted and underway. Let me say that again: all of the examples that were given to you by the government are examples

that are covered by the provisions, currently, of FIPPA. For example, with respect to the homeless intervention project, this office was consulted. That particular project was authorized under section 33.2(k) as a research project, under FIPPA, and is underway.

With respect to the tragic circumstances where the woman was shot five times but was not advised by police of the criminal record that her husband had dating back five years against former partners and family members, the disclosure, depending on the circumstances, would be authorized under FIPPA either as a "consistent purpose" or as "necessary" based on compelling circumstances. The reference there is to section 33 of the act.

The downtown Vancouver community court…. That project is one where the office was consulted and the project was authorized as an integrated program or activity under the act.

The Ministry of Health's performance evaluation of health care outcomes, the family practice initiative, so-called…. The reference was that it took nine months to negotiate and two days to collect the data. The office was not consulted in respect of that initiative, but the lesson is how easy it is to permanently link and to share data. It's a relief to hear, in a sense, that so much thought went into the project — in this case, nine months — before the linking and the sharing actually occurred. Had the office been consulted, I'd like to think that it wouldn't have taken nine months to negotiate. But the machinery's there. The enabling legislation exists. The contact didn't occur.

The use of social media websites such as Twitter and Facebook…. Section 33.1 of the act allows the minister by order to allow disclosures outside of Canada in specific circumstances and subject to any restrictions the minister considers advisable. In this case, the minister was in touch with the office, a useful discussion was held, and ultimately the minister on December 17, 2009, issued an order, M030, which permitted the use of social media sites.

The examples provided in our review are not provided in order to try to embarrass the submissions you've already received but to show you that FIPPA does work rather than does not work, as has been suggested. They do, however, serve to illustrate the lack of training and the understanding of public servants and the need for leadership and direction within the government.

That brings us back to the recommendation which I referred to earlier of the appointment of a chief privacy officer who could provide expertise and consistent advice to program areas on the appropriate application of FIPPA.

Mr. Chairman, given the time constraints and, I know, the desire of the members to engage, I'm not going to want to spend much time talking about principle-based approaches as opposed to rule-based approaches and that sort of thing. I'm only

going to say that this office has looked and looks on a continual basis at both of those kinds of approaches.

There's an old story where the Lord Chief Justice of England is talking to the Archbishop of Canterbury, and the Archbishop of Canterbury makes it clear that his job is the saving of souls. The Lord Chief Justice of England says that his job is to impose sentences on people. After the discussion carries on for a little while, the Lord Chief Justice of England finally says: "Well, Your Grace, when you tell people that their souls have been saved, they believe it. When I tell people that a person is to be taken out and hanged, he gets hanged."

I don't mean to trivialize this. Rules assist people with an understanding of what the rule of law actually is. If you don't understand what the rule is, it's hard for you to be able to adhere to the law. The principle of privacy and disclosures and exceptions and so on needs to be, in my respectful submission, so adequately and precisely defined that people know what their rights are and don't have to ultimately litigate what pious expressions of privacy and so on mean in legislation of the type that's supposed to protect people.

FIPPA has a series of clear, albeit sometimes complicated, rules, but you know what the rules are.

There was an interesting reference to Australia and the experience of that country, which is an experience that we admire. I noted in the government's submission that the submission to you was that the government wanted to ensure that there be "the right information to the right people at the right time."

When I look at the data-matching material that Australia has published recently, I note that they say that their goal is "the right information to the right people for the right reason in the right way at the right time."

So I adopt the interlineations. I think "for the right reason and in the right way," which may have been intended in the government submission but wasn't there, is the key to what it is that we have to do going forward to make sure that FIPPA remains strongly in place.

Now, on the question of the understandability of FIPPA, changing the statutory rules, in my submission, around the definition of what's called in the act as integrated programs or activities will not solve the problem of the lack of employee understanding of the FIPPA rules.

Dealing with emergency situations. The government's use of emergency situations as illustrations of the complexity of FIPPA serves to prove the point that it's a lack of training that is indeed at the heart of the problem. In 2008 there were a series of incidents at colleges and universities in both British Columbia and Ontario where parents were not advised of serious health risks to their children because

universities believed that they were prohibited by FIPPA from disclosing this information to parents.

In response, in cooperation with our Ontario colleagues, the office produced a document entitled *Practice Tool for Exercising Discretion: Emergency Disclosure of Personal Information* for universities and colleges, and a copy of that document we can make available to you. That learning tool, that exposition, has been valuable and is illustrative of how, with that kind of information provided, people on line have a better understanding of what flexibility they have and what their obligations are.

The preliminary analysis that we have done is that if the government's recommendations to you were to be adopted, virtually every other regarding collection and disclosure would become meaningless because of the broad "principle-based approach" that are contained in their proposed amendments. That would mean that at any time a public servant believed that their office or organization had a shared interest in some program or activity of another body, including non-public bodies, data should be collected and disclosed, linked and studied.

The reach of that is, at first impression and on its face, I suggest, troubling. It's not going to be the case that that public servant would be the envy of any of us in this room, having to make such a decision if they had the power to make it. In my respectful submission, it's too much authority to place in those hands.

The written submissions, which, I note, are in the executive summary to the government's submission — they're at page iii — make clear that it's the documentation and careful study that's being avoided by the recommendations: "Recognizing the range and scope of potential common or integrated programs of activities to meet and serve the needs of citizens, not limited to programs or activities with structural arrangements but rather based on delivery of a common or integrated function." In other words, the test would be "the scope of potential common or integrated programs of activities to meet and serve the needs of citizens," and that test, in my view, is not the appropriate one.

Finally, the issue about obtaining personal information based on consent. It's true that FIPPA does not authorize collection of personal information if it's permitted by statute, necessary for law enforcement or directly related to and necessary for an operating program or activity.

That section, section 26, is consistent with every other common-law province in Canada and with the federal Privacy Act. To be clear, no privacy statute in Canada permits public bodies to collect personal information based on consent. Consent-based collection is not permitted because of a very strong public policy decision that there is a significant imbalance of power between a public body and an individual citizen.

In the private sector context you seek a service from an organization. If they ask you to consent to the collection of personal information, you can choose to go elsewhere for the service if you don't wish to consent. In the public sector there's nowhere else to go. If you don't consent, you don't get the service. Therefore, consent isn't really meaningful in that context.

The current requirement in FIPPA that collection be directly related to and necessary for an operating program or activity introduces the concept of proportionality into the collection of personal information. In other words, it prevents public bodies from collecting excessive amounts of personal information "just in case," and it limits the collection to the minimum necessary to accomplish the purpose. The longstanding principles of necessity and proportionality are essential to the protection of privacy and other change in these internationally accepted principles.

Mr. Chair, at the point of concluding my remarks, I note that in all of the material — and there's a mass of it, as you've seen — a paradox is emerging in the landscape of those people who control and have personal information about people. The paradox is this. Some few years ago large corporations and multinational entities, organizations that have no altruism except to the extent that it contributes to the bottom line, could cynically be thought of as being people who were not prepared to invest a dime in protecting privacy. That was for others.

What has happened is that over the last ten years, every such major corporation or entity has invested millions — I'm now going to say tens and hundreds of millions of dollars — in appointing chief privacy officers, in making sure that the information that they receive from their customers remains safe and in circumstances where it can't be exchanged, except under rigid terms, with other entities. That devotion to training, that ingenuity, is not something that many people might have been able to predict ten years ago.

At the same time — and here's the paradox — there seems to be a resistance. Maybe it's simply my perception, but if there is a resistance to appointing chief privacy officers, to making sure that all of this sort of thing gets exchanged based on the rules that we've had for so long and that are so valuable, we're not seeing the same kind of response coming from the public sector. In a sense, we're going in a different kind of direction, or we appear to be.

It brings to mind, of course, the old story of the two moose hunters who go and shoot a moose. They're dragging the animal out of the forest by its tail, and the game warden comes upon them and says: "Do you have licences?"

They do, and he says to them: "Don't you think it would be a lot easier if you got on either side of the antlers of the moose and pulled it out of the forest that way?" They discussed that for a moment and said: "Okay, let's try that." So they did, and after about ten minutes one of them turned to the other and said: "You know, that fellow

was right. This is a much easier way of doing it." The other guy said: "Yeah, but we're getting further and further away from the truck."

Mr. Chair, I hope you won't mind that reference, but it does to some extent seem apposite. Thank you for listening to me. My colleagues and I are prepared to answer any and all of your questions. As you will appreciate, I won't have had an opportunity in the weeks that I've been acting in this position to have a fairly good grip on the operating side of things. So those questions will likely be answered by my colleagues. Thank you for your patience.

R. Cantelon (Chair): Well, thank you very much, Mr. Fraser, for a very…. We appreciate your approach with the little bit of levity. It certainly…. As we embark on very, very heavy and intense discussions, we'll need to keep an even keel as we proceed to discuss these matters.

I just want to make one comment, because I have from my government side some knowledge of the beginnings of the integrated case management system. I want to assure the office and the officers that indeed, basically, it is far from an off-the-shelf. Were it only so easy. They dream it would be that easy. It is not.

Basically, it's an Oracle-based platform of a very broad capability on which they build the capacity to do individual programs and handle the various requests of the ministries. Indeed, it's at the beginning stages of developing those programs. But it would be very appropriate to remind them of the requirement for the privacy assessment impact as they proceed with developing it. It's far from too late.

If I may briefly…. I can also recall many, many years ago — we're not quite of the same vintage but pretty much — that when social insurance numbers were introduced, we were given great assurance that they would never be used for personal identification, that they would be a private matter. Of course, we know where that is.

I have Eric Foster. What I will do is go back and forth on both sides, if I can, Members. We have about an hour and a half for questions.

E. Foster: Mr. Fraser, thank you so much for your submission.

I have some concerns when you talk about…. You talked about a couple of cases — certainly the tragic case where the woman was shot. In your submission you said that that circumstance is covered under the act. It's an emergency situation. Then a little later on in your submission you suggested that you didn't want to give the public servant that much leeway to make decisions. I guess all these things can be discussed, certainly, at this table and other tables.

At the end of the day, if we look at the sharing of information at the street level where ultimately all of this has to work, you're asking in that situation a policeman or

a social worker to make decisions, transferring information, and they're erring on the side of caution to protect their own jobs.

I think that it is too difficult. I like the idea of the training, but at the same time you're going to ask someone at the street level to make those decisions. When they make those decisions, two people are going to stand in front of a judge and argue for a month over whether they made the right decision or not. You're asking that person in that situation with limited training to make that decision in a split second.

My question is: how do we uncomplicated this at the street level? At this level and at your level, in those discussions, it is complicated — there's no question — and we have all of the time in the world to discuss it.

At the street level, be it a social worker or a policeman or anyone else that's working at that level, they have to make that decision immediately. If they make the wrong decision, people die. Then you look back on it and can say: "Well, the act would have allowed them to do it." They don't know that. They're calling in on the radio, and whoever's in charge is saying: "Well, gee, I don't know if you can say that."

To have a privacy commissioner is fine, but you can't call him at three o'clock in the morning and say, "Look, can we do this, or should we do that." I think that we've got to find a way from the privacy end of this thing. We've got to protect children. We've got to protect those most vulnerable. We can't do it if we tie everybody's hands. Some way we've got to be able to get this to the street, and I put that back to you. How do we do that?

P. Fraser: My colleagues may in fact be aware of some programs of collaboration which now exist that they can allude to in a moment. I'm going to speak very generally. I don't know, frankly, to what extent police forces teach members — let’s deal with that kind of situation — what the options are. I would have to think that there is some form of formal training.

I would also say at once that I am quite sure that as good as that training might be, not every situation could be contemplated. I understand that. But understanding that there are, if you like, with every situation results that can be shared and used going forward, it would seem to me that compilations could easily be done of particular situations, and you could produce, reasonably quickly, a guide that would be understandable and specific, covering a wide variety of circumstances.

If there was ever a need, if you like, for a chief privacy officer to be in place in any organization, it would have to be in an organization that deals with emergency situations. So all of the effort, it seems to me, should be concentrated in that direction right away. The office is, I can say, eager to help in that respect.

We are not a stakeholder in the classic sense, where people come in and say they have a stake in what's going on. We're a regulator, but the conscience of the office

is that we want to regulate effectively in circumstances where what we do and what we say and what we prescribe make sense on the street.

Any overture from any emergency force that has concerns, both specific or general, would be welcomed in the office. Within the limit of our resources, I have no doubt that we can put people together. It's a genuine offer.

D. Routley (Deputy Chair): Thank you very much, Mr. Fraser. I really appreciate your presentation.

I'd like to work backwards through the paradox that you've detailed. You've noted that in the private sector millions are being spent and invested by companies in order to create the offices of privacy officers or regulators and extensive investment in training is being undertaken.

A recent privacy conference in Victoria really underlined that for me, that the companies that are sharing information are being very, very careful about how they structure their organizations and how they ensure that they're accountable for the training of their employees.

Then we look at the other side of the paradox — that is, that the government, which is to be the leader in a sense in setting the tone and the requirement and the level of the bar where those corporations must protect privacy at, seems to be resisting the same kind of movement forward in terms of advancing the organization's capacity to understand the legislation and to apply it.

The integrated case management system is an example of, maybe, what the motive is. Not wanting to assign a nefarious motive, but just the practicality of government wanting to achieve its goals is perhaps streamlined by a really broad mining of personal information.

It also brings up potentially horrible consequences for people, some of whom you've mentioned — those people who are vulnerable, those people who have received assistance, the medical records, family counselling records of non-profit organizations. All sorts of potential breaches of people's privacy that could have quite devastating personal and financial and professional outcomes for them are made possible by that system.

In the private sector I can go to Bell for my cell phone, and if I don't like them, I can then go to Rogers for my cell phone. Then I can go to TELUS for my cell phone. But I don't give them all permission to share everything about my cell phone record with each other into perpetuity.

I think we as government are setting the bar and drawing the lines for the private sector. They are meeting the lines that have been drawn, and we seem to be pulling back form them. Is it your opinion — now I'm asking for your opinion here — that if we don't maintain our vigilance in observing these rules and maintaining their effect

that we can expect that the private sector would follow suit and abandon that broad-scale investment in protecting people's privacy?

P. Fraser: Well, I think that the private sector has done what it's done simply because there is a level of expectation among their customers that they have to cater to and satisfy.

The paradox is, from my point of view, that that same level of expectation exists in people with respect to their dealings with the government. The private sector's advances aren't likely, it seems to me, to recede. They're likely to increase, as they can market the fact that their ability to keep information safe avoids difficult moments that occur from time to time, where there have been security leaks and so on. That tarnishes the image of their company to such an extent that the company could actually be, potentially, driven out of business.

I think the private organization impetus and their initiatives will inevitably continue and get better. I don't want to leave the impression that I think the government is unmoved by the recommendations that we have made — for example, about a chief privacy officer.

As you know, the studies that I referred to were studies that involved, at least in respect of the 1,400 folks that had their information taken away from the worksite…. That study on our part was but one study. The various ministries did their own studies.

The government itself said, in a report that the chief information officer made, that the government had taken note of the fact that there should be some central authorizing or information post and that that could be in his office.

Our report, in response to that, said: "No problem with his ability and dedication and so on, but it seems to us that it would be better to take it from that realm and into the special realm of a chief privacy officer, who would be available for that particular purpose, realizing that the chief information officer has many, many other responsibilities pan-government."

If the chief privacy officer were available as a resource for the pan-government scene, if you like, and had an executive position sufficient to be able to adequately resource the office, that particular person could lead the effort to not only tell people what the law is and how they can access it but get involved in the kinds of training that we're talking about.

That's why we said…. If you like, using this metaphor, that's the bright light. That's the person that everybody in every ministry called upon as a public service to have to make decisions in difficult circumstances where they are unsure of what they can disclose and what they can't and whether, if you like, the privacy provisions are a sword or a shield. That's the person you can go to.

I know that that recommendation is under consideration, and I'm hoping that it will be ultimately accepted.

So that's where I see part of the solution being, on the government side.

D. Routley (Deputy Chair): Just as a follow-up, Mr. Chair. I appreciate that and that the training is so essential to applying the standards of the act. But you referenced that if the government's proposal were adopted, it would essentially make protection of privacy and all the other aspects of the statutes ineffective.

At that same privacy conference in Victoria we heard about a study where people rated the protection of their personal information as…. Above 80 percent of people said it was one of the top three priorities in their dealings with the private sector and government. But, almost the same percentage — over 70 percent of people — were shown to be willing to trade their social insurance number and other personal elements of their information for free chocolate.

While all the members of the public are not here reading your submission and understanding broadly and deeply the implications of the loss of privacy and of our role in protecting it, even though the private sector is beholden to their dollars and needs to market to them to say that "we are safeguardians of your information," if we, who apply regulation, don't take an approach that meets a higher standard, if we allow ourselves to share information in such a way that obliterates the protection of privacy, I wonder: can we expect the private sector, then, to follow suit? Because essentially, in the end, those private corporations are fighting for market share, but they're also protecting themselves from the liability that might be incurred if privacy is breached.

The liability and the responsibility is set here, under the legislation and the regulation. So in that way, don't you think that we need to reinforce our commitment to a regulated approach, a rules-based approach versus a principles-based approach and resist the temptation of expediency to bring down the barriers in privacy protection?

P. Fraser: I certainly believe that the system that we have now under FIPPA, which effectively records that you can collect information for specific purposes and have that information limited to those purposes as opposed to becoming at large, is the way we should continue to go.

I say that knowing that the act, FIPPA, is not a monolith, which means that, you know, nothing can happen to that information, that it will remain, if you like, immutable and there. It provides that there can be applications to deal with that information in various ways. Under the act, if the application is made then decisions have to be made and there's a process.

That's a process which may be inconvenient. It's a process which may involve — it certainly does — expense, but it's a process that's worth having, in my view, in

order to make sure that we keep safe the reason why the information was collected in the first place. I hope that will continue to be the law in British Columbia, that we won't simply decide….

I'm putting, I think, to one side this whole question about rules-based and all of that sort of thing, because I think it's a kind of an academic discussion that is of some interest, maybe, to academics. But we here in this room are trying to deal with how information must be disclosed; how information could, under a new set of rules, be provided by consent, where now is not or cannot; and what we do with respect to sharing information in immediate circumstances, where to not share that information could have all kinds of counterproductive results.

That's what I'm hoping the regime in British Columbia will continue to look like under FIPPA.

R. Cantelon (Chair): Thank you. We have four questions up, and I'd like to just urge all the questioners that this is your opportunity to get information out, and please make your questions as direct as you can. We'll start with Harry, and then Katrina, Mark and then Guy.

H. Bloy: Thanks for your presentation, Paul. What I wanted to ask about was recommendation No. 5 and the "require the data sharing projects for the purpose of research to be subject to a review."

You said earlier in your presentation that government has a heavy hand, because there's nowhere else to go, so the information can't be shared — or not easily — and you did talk about one project where information was allowed for sharing.

My question is…. Government introduces programs — all governments — on a regular basis, and I guess I'm talking about the social service sector. When they do these programs, universities and academics want to be able to follow the program to see if it's successful or not.

So is there no way that when people enter these programs — they could be given housing and then some education and some medical needs — they couldn't be followed over a five-year period to see if the programs actually works or not? What you're saying…. You're not prepared to do that. Is that how I understand that?

H. Morrison: Recommendation No. 5 refers to the fact that government research projects for the purposes of program evaluation are not subject to the same ethics review that similar research projects would be if they were conducted by universities or hospitals. We're just interested in having the same ethics review be conducted of those projects as you would see elsewhere.

The thought is that there could be an arm's-length committee appointed by the government that would undertake that ethics review. We've seen that in two committees at the Ministry of Health Services — the data stewardship committee

and the PharmaNet stewardship committee. They make decisions about release of data for research purposes, and they do include some confirmation that there has been an ethics review of the research proposals. So it's just to have that same kind of ethics review with respect to other research projects conducted by government for program evaluation purposes.

H. Bloy: Would you do that without the person's knowledge — that entered the program — or do you have to get a sign-off on each person who has entered a program — for the research?

H. Morrison: It can be done without the person's knowledge.

K. Conroy: Thank you, Mr. Fraser and all of you for the information, and I want to thank you for clarifying the information we received last week, that the case studies are in fact covered under the act. That was enlightening.

I wanted to clarify your recommendation about the government privacy officer. We have the chief information officer now, and we have the position that you're filling right now. So you're asking for another body to be….

Assuming you're asking that to be an independent person, an independent officer, if that person was in fact a government position, so to speak, the potential to be co-opted into protecting government privacy instead of actually protecting the public's privacy or information-sharing could potentially happen. It could happen in any government, and I'm just wondering where the thought is on this position — if it is, in fact, an independent body or if it is a government position.

C. Tully: The recommendation with respect to a chief privacy officer was intended to be an appointee of the government, a lead within government. We already serve the function in terms of regulating information and privacy under the act, so we're not suggesting that that needs to be hived off of our responsibility. This office is the office of the independent officer of the Legislature.

So indeed, we did think that the chief privacy officer should be part of government, should provide that kind of internal expert advice and guidance, lead the training, be the place where employees can go and be comfortable — that this is part of government, they're getting the government position. They can weigh the interests of government, of course, but also be an expert on privacy and help the government to understand how to comply with FIPPA and accomplish their purposes.

K. Conroy: So just to clarify. This is something that the chief information officer now would not be doing.

C. Tully: Well....

P. Fraser: I don't know what that job description is, but my guess is that you could put that in the basket of responsibilities that that person has.

I guess the practical reality, from our point of view, is that that's a huge responsibility — to be in charge of IT across the government and try to deal with all of those issues. We had more in mind a situation where there would be an employee of the government who would simply be the person that you call for information and, if you like, some advice. That person would be identified in all of the ministries, and presumably would have contacts himself or herself in the various ministries, so there would be a network of people who would be concerned specifically about privacy issues and responses.

We thought that it would be most efficient if it was a new hire, if you like, and someone who would have that dedicated responsibility — privacy being, we think, a uniquely important issue and not one that should simply be but a part of the larger IT world. That was the basis for the recommendation.

I have to say that there's nothing most people admire more than an opinion they share. A lot of private companies have chief privacy officers who coexist, it seems, with IT departments and who may be involved in what I would guess is a dynamic tension not infrequently, as IT people want to come in any say, "Well look, we can save some money here or cut a corner there," or whatever. You've got someone whose dedicated responsibility is in the privacy sphere.

To that extent, imitation is a form of flattery in terms of our recommendation.

R. Cantelon (Chair): We're certainly familiar dynamic tension within the walls of this house. Marc Dalton?

M. Dalton: First of all, thank you very much for your presentation. It's very helpful. Thank you for your comments.

Just in the area of education — I wonder if you could make some comments regarding BCeSIS, the information system used in the educational field from K to 12. Comments on that, but, more particularly, the recommendation and possibility of developing an EDI, educational development index, for children from birth to five years old in order to track children to determine vulnerability and to assist in their educational development. Could you comment on that, please.

P. Fraser: One of the things that people in your position need to be sure of is that people in my position don't tell you much more than they actually know. I'm bound to say, therefore, that I'm going to ask one of my colleagues to respond, because I really can't answer your question. If any of you can, please go ahead.

C. Tully: I think I understand your question to be whether or not, say, the ministry.... You haven't specified who would do this, but to develop some sort of index to evaluate risks to children, say, from kindergarten to five years old.

M. Dalton: No, from birth to five years of age — to kindergarten age. Their developmental index, whether it be health, education. It's been recommended by

HELP, I believe it's in the *15 by 15* report, to develop this type of system in order to track at-risk children and vulnerability.

C. Tully: You know, this would be the kind of project that would need to go through the analysis. Most likely, if it were to occur, in terms of disclosure, it would need to be an integrated program or activity.

What we've said in our submissions, and what we've been saying for the last three years about that existing section of FIPPA, is that you need to build a structure around that kind of project, setting out what the purposes are, what information you intend to share, what the roles of each of the partners were.

So is it possible within FIPPA? It is possible within FIPPA. It takes work, and it takes thought to make it work.

I think that's the answer. Without more information, I could never say positively one way or the other. It could definitely be designed to fit within FIPPA and to track these children.

You know, sometimes the answer under FIPPA is no, but no to, maybe, this and yes to this.

G. Gentner: Thank you, Mr. Fraser, and your staff for providing us with the information.

I was listening to every word, and I'm hopeful that we will be able to call you back, because I don't intend to do a psychoanalysis of what you said, but I do want to go back and read every word. I think it was very thoughtful and somewhat inspiring. There's a lot of meat there that I would like to digest.

Having said that, I can tell you that the world is changing, and we should be reviewing not only the act but the means. I agree that we have to have — I won't say a police person — somebody who is empowered. I also look at some of your recommendations where the commissioner should be giving more authority to look at some of the orders and complaints. I find that we don't really have the policing of government that has refused to deal with section 13, for example.

There are some things here that I find have not been addressed. I could, first of all, talk about the changing world. I can buy an ad in the *Tyee* knowing what audience it's going to, but if I was to go to Google, everybody's profile when you hit the send button, that's where we're going. Profiling is a dangerous part of the new business, and I suppose, in many ways…. Talking to my younger children, they've accepted it. But I guess me being more of the fuddy-duddy, I really worry about the loss of my identity and the new Big Brother media out there or world that is able to profile us.

I find, though, Mr. Chair, that I like to know — it's been brought to our attention many times — the prohibition of information based on the fee structure when you

apply for freedom of information, FOIs. I know there are some recommendations here, in specific No. 12, where you talk about free of charge on finding personal information, but there seems to be many barriers in the way to just finding general information. I know we can talk about the routine information that should be available.

I don't know, maybe I've missed it in the recommendations, what the office's position is of making it more transparent, open, and tearing down those barriers of fee structures. That's one. And, too, you talk about the need to have more authority to review and mediate, and yet we look at what, again on section 13…. How can you expect the government to change the act to give you more of the intervention aspect when it refuses to deal with the necessary changes to amending section 13(1)?

I know those are loaded questions, but we have limited time.

C. Tully: With respect to the fee structure, we've tried to make recommendations to reduce the number of times you have to make a formal access request. We feel that this will have a significant effect. It's more timely, it's cheaper for the government, and it's cheaper for applicants. So the electronic reading rooms is another way of dealing with the fee issue. The fee structure itself is quite old.

We had a look at our statistics just to see how often the fees come up as an issue. I think we were in the range of just 36 fee complaint files in the last year. The average fee in those was $1,400. And in 64 percent of the cases, the fees were reduced or waived as a result of our negotiations with the parties.

Honestly, part of my answer comes from the fact that I worked in a public body for five years and assessed these fees. Part of the challenge for public bodies, I believe, is that they are estimating fees. It is part of the process. Originally, they estimate the fees. When they are finished processing the request then they make a final count of the fees. We're back a bit to that training issue of learning to properly estimate the fees so that they are accurate from the start.

The second training issue is with respect to fee waivers, the individuals tasked with making decisions about fee waivers also need to keep current with the case law on evaluating whether a fee waiver should be granted or not.

I'm not sure if that answers your question, but we haven't made a recommendation with respect to actual regulation and setting the amount of fees. It seems to us, certainly, that fees should not be a barrier, that access is a right. But, to a certain extent, the act chooses to allow for fees.

G. Gentner: Just a quick follow-up. Are there no recommendations on how we can streamline it so that it is not so costly? We have heard many of your submissions, and I gather here from Paul's position that streamlining would make data easier to access. If there was a template put in place where it's automatic, that it's at your

fingertips…. We're in a fingertip type of world. Is there some kind of system that you can recommend that we adopt and not infringe on privacy?

C. Tully: We did recommend that where the records are electronic, in response to access requests, they be released electronically, which would be quicker and less costly.

G. Gentner: My concern on section 13…. I know those are recommendations. That's going back to 2004. Basically, you are continuing with those recommendations.

C. Tully: We refresh that recommendation looking at what has happened since that time and discussing some of the more recent court cases to support our position that the original intention of section 13 should be renewed with the recommendation from this committee.

J. Kwan: Thank you to Mr. Fraser and his delegation for the information that they have brought forward today. It is indeed good to know and for all of us to understand that the existing provisions within the act already allow for government agencies to access the necessary information, in particular, the cases where issues of safety and concerns, as such, are at issue. So it is very good to know that.

In the presentation last time from the Ministry of Citizens' Services on behalf of the government, they also asked the committee to consider, you know, these broad, sweeping changes to facilitate access to information across agencies within government. The proposal was so that they can enhance their ability to do work and to facilitate and provide for services and benefits to citizens. It was sort of cast in that light, and some of those particular examples that were highlighted and responded to by Mr. Fraser were addressed today.

In terms of the overall thrust of that request, my understanding was that the request was going to be applicable not for a selective group of individuals where cases of health and safety might be related, but really it would apply to virtually anyone where the government deems that exchange of information would be necessary.

So I would like, I guess, anybody on the panel here today to respond to that aspect of it and the concerns, if any, that you might have related to that request.

P. Fraser: Thank you for the question. The clear sense that I have is that the suggestion is that the new order of things would allow people to consent to information being given. It would then be at large and available across the government, and there would be no front-end process that would limit the request in any way to a particular purpose and for a particular reason that would simply allow government to share across its various ministries information that it has in circumstances where the information could be retrieved by any number of recipients for their purposes.

The fundamental difference, as I think I understand it, is that FIPPA, from my interpretive point of view, prohibits that kind of conduct. Indeed, that's basically one of the principles of FIPPA. One of the international principles is that information should be collected that's personal only for specific reasons and used for those specific reasons, and that otherwise it shouldn't be accessible.

R. Sultan: As the others, I'd like to also thank you, Mr. Fraser, for your very thoughtful remarks.

I have two questions. The first is it seemed to me that the tenor of some of the questions and responses this morning would lead one to conclude that perhaps the FOI aspects of this position are separate from and in some ways contradictory to the privacy obligations of the position.

If that is true — and it seems to me there's an element of reality there — and if at the same time the government is appointing or has appointed or is in the process of finding a chief information officer, could we contemplate the restructuring of this office so that the FOI aspects are a responsibility of the chief information officer, just as the health authorities are expected to deal with people who are wheeled up in an ambulance at the hospitals? Just another part of the job. And if they aren't doing their job, they have the normal political recourse to the MLAs, etc.

The privacy aspects are so sensitive, so broad and in many ways adversarial to government instincts that they really, I think, could justify a singular focus, all by themselves. Does that make any sense?

P. Fraser: Yes, it does. At first impression, one would say: "Well, privacy and access are counterintuitive, and how can they live under the same roof?" And indeed, we've seen in experience across the country, in the federal scene, particularly, that those responsibilities have been severed and have been populated by different people from time to time. In the rest of Canada, in the provinces, maybe for some expedient purposes — I don't know — we have a different regime where, under the same roof, you've got people who are making those decisions on either side of the information issue.

I'm going to ask Catherine to comment on that in a moment. The only other thing I would want to say is that, looking at the landscape that you've described, we should just be clear about who the players are.

The Information and Privacy Commissioner, of course, is, as you know, an officer of the Legislative Assembly and so is independent in that sense. The chief information officer, who is in place, is in the employ of "the government" and appears to be the person who is in charge of the government's strategy in terms of dealing with the kinds of issues that ultimately we encounter in FIPPA. The chief privacy officer, as we've been discussing, is but a recommendation but would also be a government employee.

So those are the three positions which we've been discussing. Catherine, I think, can explain to you better than can I how the apparent incongruity of the access and privacy situation appears, nevertheless, to have been working in this province and in all other provinces.

C. Tully: Our role under the act really is to interpret the act, and we have a variety of processes to decide whether or not a public body has satisfied the rules under the act.

There isn't really any conflict between the access and privacy rules. It's just a matter of determining, you know... Somebody comes in and claims that a public body failed to respond to an access request or severed incorrectly. We have a look at that. We look at the rules. We look at the case law, and we give an opinion in the course of mediation. If that isn't satisfied, it proceeds to an inquiry.

On the privacy side we can have public bodies coming to us to comment on the implications for privacy of a system. We look at the rules. We evaluate the case law. We look at what they're proposing, and we comment on the system. No conflict arises in that. In terms of a chief privacy officer, though, in government, they will be in the position where there are a lot of things pulling at them.

There are the privacy rules that they're trying to interpret on behalf of government. But government has a lot of other interests, and there are a lot other public interests that need to be weighed into how they interpret and apply the act. So they will be in a position where their main goal will be to protect privacy, you know, in the context of allowing government to achieve its goals.

In terms of the access side of government's role, I don't actually see a conflict, really, with the goal of access in terms of individuals requesting access. But there is a conflict where they're trying to share information for program delivery. That's why it's helpful on the government side to have somebody who's got a clear focus and expertise on privacy so it can assist and guide government.

On the commissioner's side I suspect but don't know that the division between access and privacy commissioners at the federal level was really a matter of caseload and the amount of work required on each side as opposed to any view that those functions need to be separated. I don't know that for certain, but as Paul mentioned, across Canada at the provincial level all of the commissioners' offices have both responsibilities. Perhaps it's a matter of efficiency, too, of service delivery.

I don't know if Celia knows anything more about the history.

C. Francis: Well, the federal legislation.... There is a federal Privacy Act and a federal Access to Information Act, but they are intended to be read together harmoniously. The case law has established that quite a number of times. So I

agree that there is a certain tension in access and privacy, but it is possible for them to work together.

Probably the greatest tension you see is when we're interpreting the personal information protection exception under our legislation anyway. The act authorizes people to request records, gives them that right, but if it includes the personal information of other people, the decision-makers have to decide whether the access applicant is entitled to that other person's personal information, going through a number of steps under section 22 of our legislation.

That's probably another aspect of the tension we see in our work between access rights and protection of privacy rights.

P. Fraser: I'm glad to hear it described as tension, because if it was conflict, I might have to do something about it in my other job. [Laughter.]

I wanted, Mr. Sultan, as a bit of a kindness, because I think it was you that raised it with the government presenters — the issue of people who are making frivolous and vexatious demands, people who are recidivists and that sort of thing.

There is provision in the act, section 43, which you may or may not be aware of, and I don't think was noticed in the discussion. Under that section the commissioner, if the head of a public body asks the commissioner to do so, "...may authorize the public body to disregard requests...that (a) would unreasonably interfere with the operations of the public body because of the repetitious or systematic nature of the requests, or (b) are frivolous or vexatious."

That section of FIPPA, which has been there for a while, is another tool, if you like, in the toolbox.

R. Cantelon (Chair): Stephanie Cadieux had a question, so I will, if I may, put her at the head of the list and then carry on with Eric, Doug and then Guy.

R. Sultan: I was going to ask a second question.

R. Cantelon (Chair): You may ask a follow-up question. Certainly. Right now.

R. Sultan: Well, it was more of a request for a comment. I see two forces at play in our society which have already been described to some degree, but I just wonder how we can resist them.

One is the overriding necessity that we are persuaded is required for national security and the fight against terrorism. I applied for one of those FAST passes at the U.S. border a couple of years ago, and before you know it I was being fingerprinted and giving a retina scan.

Voice recognition, I'm sure, is improving. Biometrics. I now have a piece of inexpensive — in fact, free — software I downloaded from Google that will scan the thousands of electronic images I have on my camera and pick out all my relatives by face. It's quite incredible.

DNA, we all know about. Of course, we have the spectacle in the United Kingdom of — it appears, from what I read in the press, at least — a television camera on many, many street corners. Goodness knows what's happening to all that information.

Under the imperative of security, the databases of the national agencies, I'm sure, are growing exponentially — they don't talk much about it; it's a big secret — scanning the airwaves for key words. And on it goes.

It's a gargantuan machine that's in play that we only dimly perceive, but I don't see it slowing down. Of course, the implications for privacy are enormous.

The other broad, almost inexorable, force that I think we're dealing with here is social policy imperatives. As society expects government to do more and more, raising its kids and educating them and looking after us all in our old age, etc., the government does its best to cope with these things in a rational policy analytical way which requires lots of analysis of microdata, tracking individuals over time — what works, what doesn't work.

We have in Vancouver, British Columbia, for example, I think, an astonishingly effective example of research into early childhood development which has required, to my amazement, getting into the level of classroom data on individual student performance — Mr. Clyde Hertzman, is it? — all to a very laudable end. I think we're just beginning to see the beginning of it.

So how do we cope with the social imperatives and the security imperatives?

P. Fraser: Well, I guess, how long is a piece of string? It's an interesting profile that you paint. It's a generational thing, as you or somebody else pointed out. Maybe it was Guy who said that children, for example, seem to have no real proprietary interest in their own persona. If you have to do this push of that button in order to get that service, then so what? Maybe as you get older, you become more sense about your own sense of mortality and it seems more important than it does when you're 12.

Anyway, the phenomenon that we've described is, I think, accurately described. What happens to all of this information? It could, if we give up, just simply mean that it's out there and can be accessible randomly by whoever might for whatever moment be interested.

I would hope that we're all opposed to that, as a consequence, and that we're prepared to continue to do something about it, which is, at the moment, FIPPA. It

may need some customizing — and always will, because it's an act that will never, effectively, remain immutable. I understand, as I think we all do, the challenges that government faces in terms of trying to work around what it can see are clearly better-economic solutions to get to the result, but the end can't, where matters of privacy are concerned, justify the means on an open-faced basis.

Anyway, I appreciate your thoughtful comments.

R. Cantelon (Chair): We'll go to Stephanie, who hasn't had a question yet, and then I have a list of Eric, Doug, Guy and Jenny. I hope we'll have…. We should have time for all the answers. In the event we don't, please make sure you put your questions through to the Clerk, and we'll get them answered and forwarded to you. Indeed if subsequently any other questions occur to any of the members of the committee, please put them in writing to the committee, and we'll get those questions answered.

S. Cadieux: Again, I echo that. I think — if I'm hearing you correctly, and certainly it would be my personal belief and understanding — that as it is — although there are always clarifications or adjustments that need to be made for the purposes of addressing things that come up, that change in society, technology and so on, as you have laid out in your submission — the act, all in all, is a good act. It's there, and it serves its purpose, to provide for the access to information but also to protect the personal information of individuals.

When we look at the provision or the sharing of information and data across ministries within government where the intent is to provide better solutions for the end users of the programs, where in the act is the reasonableness test or the allowance for the reasonableness?

I think that as an individual…. Certainly in my own office, when I am confronted by constituents who are recipients of services in multiple areas, most of the time those individuals do not understand, if they change their address with one part of government, why another part of government doesn't start sending their cheques to that address — or these sorts of situations. They understand "government" to be one entity. They don't understand ministries that work in isolation, or silos, or where information is siloed off for the protection of those individuals.

Does it not make sense for government…? Does FOIPPA as it stands today not allow for sharing of information for specific purposes that are defined? Are we not really talking about the fact that people just are afraid or uneducated in how to make those things happen legally, with adequate protections? We're not looking to, I don't think…. Although, I think, some of the previous submissions may have suggested that we need to allow things differently, I don't think that we necessarily do.

I think we need to look at what is allowed, at why the protections are there and at how we implement those. I know from my past experience in the creation of databases and the use of them that certainly, protections can be put in place so that

people don't have access to any one, discrete piece of information that they shouldn't have access to. But where the information is the same from department to department to department, would it not make sense for there to be only one record?

P. Fraser: I suppose I'm going to ask Catherine to respond to that in the contest of the work that the office does, but it's interesting in terms of what you've just mentioned. When we did the coastal health care study, we were looking at a system which, I understand, is a so-called parasystem which has recently been adopted by, I think, the Coastal Health Authority, which is a software program that essentially wants to, if you like, pollinate information to those parts of, in this case, hospitals where the information can be useful.

The experience seems to be that — as you say, Stephanie — the software can be designed to gather, protect, hold and exchange in appropriate circumstances. That equipment is out there. It can be purchased in some cases off the shelf and in other cases custom design.

It's available. It's the question of whether or not people want to go so far as to improve it and to equip it and construct it to make sure that that happens, which is another way of basically saying that the office has long advocated for the fact that if you're going to be faced with that challenge, and it's a challenge that's quite legitimate, then you've got to bake in the privacy mechanisms at the front end.

Presumably what you've got to do, if you follow the privacy assessment drill that the act provides, is you've got to come in and show how you're going to be able to do that, and there's going to be some kind of engagement with the office.

We are the regulator, but it's not an adversarial climate that we attempt to create. There is a test of reasonableness, which I have no doubt that Catherine will refer to in various sections of the act, which means that the act contemplates that there will be a give and take of opinion and that there will have to be some room for, presumably, negotiation and so on.

FIPPA is not some kind of relic that can't respond to this need, and it is a need. Indeed, we want it to be able to respond. Essentially, what it comes down to is using the equipment and the infrastructure that's already there. Catherine can give you a more specific response to your question, I'm sure.

C. Tully: My understanding of your question is, for example, a change of address being shared across ministries. Can that happen under FIPPA? The answer is: yes, it can happen under FIPPA, in a variety of ways.

The easiest way is parallel to something that happens with income tax, on your income tax form. You consent to the use of that information for elections purposes. So whatever organization, whatever public body originally collects the change, if they have on their form a box that says, "We consent to you sharing that across to other ministries," that's the easiest method of sharing that information across.

There are other means without consent, such as consistent purpose, depending on the circumstance, or even integrated program or activity, depending on the circumstance.

Often with any one of these questions, it's a problem-solving exercise. That's how I think of it. It's a problem-solving exercise. How do you do it, and what are the requirements to get there?

R. Cantelon (Chair): We now have four questioners, and I think will pretty much fill up the time. Please make note if you have further questions.

Starting with Eric, and then Doug, and then Guy and Jenny.

E. Foster: Back to the privacy, both in the public and private sector. Although, to Ralph's comments, the optics of having the freedom of information and privacy in one title…. I liken it to being a strong advocate for pro-life and at the same time support the death penalty. That's sort of the optics of it, but I appreciate your answer, Catherine. It gives me some confidence.

We'll go back to the file of the 1,400 pieces of missing information. I wonder if the employee that did that — and we don't know, of course, because his history is protected by the privacy act…. If information on that employee was shared from a previous employer, would we maybe not be in that situation?

Having worked in the school system, we'd get phone calls about past students weekly from employers, and I was prohibited from saying anything.

If I couldn't say, "Hey, that's a great kid. You should hire him," I'm prohibited from saying anything. I can't say that he showed up late three days out of five. I can't say that he missed 15 days a semester. So then they hire that past student, and the student's of no value to them. They last about a month. They let them go because they don't show up for work. Pretty soon the phone stops ringing because I can't give that prospective employer any pertinent information.

I've heard this complaint from employers all over the place. They can't get good information about prospective employees. They're not even allowed to put on their application, "Do I have your permission to contact past employers?" anymore.

Again, I believe we've thrown the pendulum too far. We've protected this person's privacy — in these situations not at our peril but certainly at the expense of a whole other segment of society. Where is that balance?

C. Tully: I'm a little bit puzzled by your question, and maybe it comes from not your misunderstanding but the people who are designing these forms misunderstanding.

Certainly, a former employer can give information about a former employee with consent. There's no reason why a new employer who's interviewing somebody….

They say to that individual: "I need to check references. Your most recent employer is the most important one. Do you consent to me doing that?" If they don't consent…. Well you're making a hiring decision. You don't have the key information you need. Then you make your hiring decision.

They can seek consent and not get it, and that's fine. Then they make their decision. They hire this person knowing they haven't got the reference they want. You, as a former employer, would wait to receive the consent from the individual and then give the information. I really do see that it's not the obligation of the new employer to decide. If this is key information and they don't have, then make your decision accordingly.

Does that answer your question?

E. Foster: Just if I could follow up. What I'm going to do is I'm going to get you some specific case files and then we can deal with it.

C. Tully: That would be great. Specific facts would be great.

E. Foster: Absolutely. Thank you.

D. Routley (Deputy Chair): In response to that last question, I'd like to just share an experience, a casework in a neighbouring constituency, where a person had given the employer the right to ask questions about their criminal record. Information was shared that they were in a car that was stopped. The driver of the car was charged with possession of a narcotic.

Well, that person didn't get the job they were seeking. This was overturned, So it showed how sharing too much information…. As soon as you cross the line, someone can be seriously impacted by more information about them being shared than might be necessary.

My question is related to the privacy impact assessments. Your report and your presentation here recommend that a privacy impact assessment be done for the integrated case management system. You've indicated that…. Compared it to environmental assessments being done after a project is undertaken — how ridiculous that would be on the face of what we understand and expect.

There has been no privacy impact assessment yet done or at least communicated. How do we reform the act to ensure that that is an effective measure and that it happens along the timelines you've recommended? Would you recommend it be the responsibility of the chief privacy officer that you've also recommended?

P. Fraser: The recommendation in fact is recommendation 6. We add a requirement in FIPPA that privacy impact assessments must be completed at the conceptual design and implementation phases of an electronic-record project. The

requirement should apply to health authorities as well as to ministries of the government.

That's, as I mentioned, I think to correct the fact that at the moment the act doesn't have any temporal deadline or requirement. With that, it seems to me there's some real definition to when the assessments must be completed. Understand that assessments is plural in that recommendation. We're not talking about one assessment. We're talking about a process.

I should say, I think…. I don't want to take up your time, but I should say, in fairness, that the office has been consulted over the course of the last two or three years. The consultation has been brief, but the office was made aware of the fact that the project was underway or was being conceived and that progress was being made.

The request has been made by the office to provide information about the privacy framework, if it exists. That request has been delivered as recently as a month ago. I have met with some of my colleagues, with the chief information officer and with the assistant deputy minister who's in charge of this aspect of the program, in order to make it clear that we're looking forward to having this framework provided. I'm hopeful that we will get a response soon. The Chair indicated his involvement in the past, and I'm grateful to know that.

One of the concerns that I have — and I don't say it's a concern in this case, but it's a general concern — is that I have seen instances — this isn't one of them — where, effectively, equipment is blamed for inadequacies down the road; where, as it's turned out, the equipment that was in place, in terms of the software program, had the capacity, the capabilities and the ability to delivery on a privacy basis but hadn't been asked or programmed to do so.

Hence, the need at the front end to understand what the capabilities of the software system are. When you know that, then, you — I don't, but people who know what they're talking about in this area do — will be able to advise whether the equipment is of a type and of a kind that has privacy concerns easily constructed into it.

R. Cantelon (Chair): If I may, just for clarity then. It's required by the act now — the assessment — and your point, I take it, is that it be timely to be effective. Is that it?

P. Fraser: Yes. At the moment, there isn't a…

R. Cantelon (Chair): There isn't any time frame now.

P. Fraser: …time requirement.

R. Cantelon (Chair): Excuse me, Doug. Carry on.

D. Routley (Deputy Chair): Thank you. But you've also referred to it as a process, and I think at least three times you've asked for it. But I'm not clear whether you've asked for three different levels of assessment or that the assessment should be carried out before, during and after.

P. Fraser: The recommendation that we've made is that that's what would be required under the act. At the moment, what we have been talking about is simply the requirement for a description of what the privacy piece is in the software, what that portion of the software program that's devoted to privacy actually looks like. That's what we're waiting to get.

D. Routley (Deputy Chair): Just one more. In a broader sense, in examining privacy, you've referred to White Papers and Green Papers. If government were to undertake that kind of process in reviewing what British Columbians should expect and receive in terms of privacy protection, would you have a recommendation? Should there be a White Paper process?

P. Fraser: The recommendation of the White Paper process is found in the last annual report of this office. Mr. Loukidelis made that suggestion. His view, and it is also mine, is that if you're going to suggest or make plans to embark upon a project that's as big as the project that we have been discussing and that has the privacy implications that clearly would flow from that, then you have…. It's wise under those circumstances to consult with people, make sure they understand what the ramifications are and get some reaction.

Now, this idea has been around for two or three years, if you put together all the information that there is about it. Deloitte, as I mentioned, has been put in place. Presumably they're giving advice on some technical aspects of all of this. But the suggestion of a white paper wasn't taken up.

The consultative process, it seems to me, could inform this project and serve it well. It could also, it seems to me, allow people who have concerns to get answers, and those answers and what flows from them could in turn be put into the program, so that you're not going to have to effectively retrofit or attempt to retrofit or add on something down the road if it turns out that you've missed something.

The green paper idea was one that was used by governments particularly in the U.K., where formed plans hadn't been made and the government was simply trying to, if you like, do a form of political polling to see what the population was interested in supporting and making recommendations.

Many, many years ago I spent three or four years as the chair of a royal commission on pornography and prostitution, and we published, in advance of public hearings, an issues paper telling people what we thought the issues were in those areas, asking them whether they agreed and whether they had other issues to suggest. We didn't want at the end of the process to wind up in a situation where somebody would say: "Well, you missed the point. There was this big issue that

was sitting there" — now we call it an 800-pound gorilla in the corner; fortunately we never used to say those things then — "and you've missed it, and so what good is all of this?"

That paper was a useful tool in terms of helping people organize their thoughts and make submissions. That's perhaps too private a recollection, but that kind of consultative process was helpful. It seems to me generically that any time you consult, you learn.

G. Gentner: Recommendation 9, very briefly. Some of the members of this committee also sit on Public Accounts, and we had a submission from the archivist regarding the disposition of papers. For example, he came and told us…. We were wondering about the financial mechanics, so to speak, of disposition, and the archivist said they are contemplating destroying the Conversation on Health papers — which in our estimation, on this side of the House, was a complete failure — and we thought maybe it had something to do with the lack of financing to put these papers to rest.

Of course, in my view you could just put them in boxes and stack them for a while. But it brings to mind the sort of politics we deal with and reminds me of another story I have to quickly share with you with the Dominion Archivist years ago.

I was involved with the Mackenzie King papers, and the whole thing is now online. You can do a word search. You can find out everything you want to know about Mackenzie King's séances, right down to indiscretions with his dog, if you will, Pat I, II or III. The point being, of course, is that that information is available. It is so much available that I actually went further enquiry was visited by CSIS, then, of course a special division of the RCMP to investigate how I knew about some expungements of the diaries and the fact that the Rockefeller Foundation from private money was able to rescue its disposition. However, there was some tampering with the diaries.

Anyway, where I'm going with this all this, of course, is that on number 9 the recommendation is that the commissioner has a power to investigate and ensure compliance with the Document Disposal Act. Now "compliance" is an interesting word. How do you find compliance if the government's unwilling? And do we put penalties? Is there litigation? Is this a criminal matter, the disposition of information, or are you just a watchdog wagging your tail?

P. Fraser: Well, Catherine, are you able to respond to that?

R. Cantelon (Chair): You don't have to respond to the Mackenzie King part.

P. Fraser: I guess it was the combination of the references to King's dogs and our being the watchdog that really put me off.

C. Tully: Under the Document Disposal Act, the government is required only to destroy records in accordance with approved schedules. What we've done is had a

look at what's happening — provisions in the Alberta Freedom of Information and Protection of Privacy Act — and thought it might be something of use in British Columbia to have our office in a position to comment on and evaluate whether or not destruction has occurred in accordance with the approved schedules, to try to give the public an opportunity or an avenue to complain about the improper destruction of records.

We haven't made any recommendations with respect exactly to outcomes or consequences. Generally, our approach is remedial, not punitive. That is, the point is to make the act work to make records accessible, to help public bodies and organizations comply with the act so that the documents are there. So I would assume that we would…. We haven't talked through exactly what the outcomes would be if we were to find an inappropriate destruction of records. That would be something, I think, for further discussion.

R. Cantelon (Chair): Thank you. We'll move to the last question, from Jenny.

Before I do, I want to tell the members that we're going to compile binders of all of the submissions made, in a summary form as well. In that, also, there'll be a matrix where we sort of outline the issue by issue and what each group or presentation said, to try and frame and guide our recommendations. Because it's going to be a very onerous task. It's at least, probably, two full days, so I charge this committee now to be prepared for that. There's no easy way out of this, and it's going to take some time to do this and do this properly. It's a very, very significant challenge we have.

With that, I turn to Jenny Kwan. Yes, Mr. Fraser.

P. Fraser: I just wanted to correct the record. The recommendation that was made with respect to consultation, which is recommendation 2, reads: "Government should not proceed with any more data-sharing initiatives until a meaningful public consultation process has occurred and the outcome of that process is an enforceable code of practice for data-sharing programs."

My answer a moment ago could easily be interpreted to mean that the consultation process would be targeted only for this one program which we've been discussing. In fact, it's a general recommendation having to do with data-sharing initiatives.

R. Cantelon (Chair): A broader framework, in other words.

J. Kwan: I'm operating in slo-mo today. I'm still trying to wrap my brain around the fact that the proposal came before the committee from government without even initial discussions with your office to sort of get some insights from your office around the proposed changes. That is just astounding to me; I have to say that. And I have not been able to get over that point.

Having said that, your recommendations are appreciated. Your presentation is appreciated as well. There will be long deliberations, no doubt, around this issue.

Now, on the question that I asked you earlier, Mr. Fraser, you responded that on the consent of the people in terms of the data sharing…. You still then cited issues of concern as they pertained to the act.

My recollection of the presentation from the government representatives last time…. The extent of revamping the act would apply to individuals who have not consented as well. Because we actually engaged in that dialogue as well. There was the question: is it meant to be for people who they aim to provide assistance to, and therefore, consent is sought, or is it broader than that? It was actually both. I just wanted to clarify that point from my perspective.

The follow-up question that I have ties a little bit into what Guy Gentner was raising, and it is in this context. I'm wondering whether or not you have any thoughts or recommendations related to the issue of to what extent government should be allowed to challenge the decisions of your office — in other words, court action — to which, I understand, there court actions initiated and so on. Do you have any thoughts on that aspect of it?

Along with that, do you know of other jurisdictions who.... How have they handled those kinds of issues in their own provinces or in other jurisdictions?

P. Fraser: Well, dealing with the first part of it — the relationship that the office has with the government is, as I've said before, one of regulation. We are regulators, not stakeholders, and because we are regulators, we are enforcing an act. From our point of view, the compliance with the act is essentially our *raison d'état.* It's our mandate.

The act is open, obviously, to being interpreted. The act is the instrument of legislative draughtsmen who attempt to capture the intent of the legislature at the time that the legislation is passed. There are going to be, inevitably, it seems to me, in that process, differences of opinion as to what a proper interpretation is of a particular section. We've had a brief discussion today about section 13, for example.

Litigation sometimes follows. I don't resent that or fuss about it. There have been occasions when, as a result of that litigation, the resources of the office have been compromised, and where that has happened, the special committee of the House that deals with the public accounts, or at least the budgets for the commissioners, has catered to that. This office, in this past year, received funds effectively for the purpose of funding that litigation.

Inevitably, the plaintiff in that kind of litigation is going to be the government, in the way in which our process typically works. That's just a consequence and a cost of doing business, as far as I'm concerned.

I don't know whether there's been any experience across the country that could particularly inform the rest of your question. I don't know whether we're more or less litigious here in British Columbia than we are elsewhere. I'm sorry. I just don't have that information.

J. Kwan: I'll just follow up with a comment on that. It would seem to me, in the case where it's the government challenging your office, at the end of the day, the pool sort of comes from the same place — that being taxpayers — for these kinds of litigations.

I'm not wondering.... Is there another approach through which we could come to resolution in a more amicable, effective and efficient way that actually saves taxpayers' money? I'm sure that that money could be well spent on both sides, in terms of legal representation, somewhere else within government services. Hence, I ask that question to see whether or not there is some other possible mechanism that we could deploy to avoid this kind of situation.

I fully understand that, from time to time, such is the nature of all of our work, I suppose, that there would be differences of opinion. Somewhere along the way, I guess, there needs to be an arbiter, if you will, to resolve that. But at the same time, I am wondering if there's some other mechanism. Perhaps that's something that is worth the committee's while to look into — some other possible options.

R. Cantelon (Chair): That's a useful suggestion. I'd like to thank Paul Fraser and your group to make yourself available. I thank you for the information.

I want to, first, apologize that we didn't deliver the government's information to you directly, but I would now invite you.... If you wish to make further specific responses to all the government recommendations, we would circulate them, and that could be very useful as we move forward if there are some questions that you wish to further expand on.

I'd like to thank the committee members. We're finishing nearly on time, and I appreciate their work in doing that.

With that, we have a large task ahead of us. Thank you for coming, and thank you for setting a tone, which as Chair I'll try to emulate and hope to proceed as we move into discussions among ourselves. I hope I should be so fortunate as to maintain that tone. So thank you for coming.

H. Bloy: I move adjournment.

D. Routley (Deputy Chair): Mr. Chair, I just wanted to let the other members of the committee know that the Freedom of Information and Privacy Association released a report today, which members might be interested in. It's *Culture of Care or Culture of Surveillance*. It's related to the subjects we've talked about — integrated case management.

R. Cantelon (Chair): Thank you for bringing that to our attention, and please submit it to the committee, and we'll circulate it to all the members. That would be of interest to us.

Motion approved.

The committee adjourned at 12:06 p.m.

[Return to: Committee Home Page]