personal information banks, which would be directories that contain personal information. In four of the jurisdictions a document has to be published that contains general information regarding the types of documents that are used that are in the possession of public bodies.

The third question asked for information regarding the timelines for access requests and inquiries, and the charts on pages 13 and 16 of the document show these timelines. One clarification that should be made with respect to these charts is that British Columbia's legislation defines "day" as excluding weekends and holidays, so even though there is a 30-day period and a 90-day period, the timelines in B.C. would be longer than a jurisdiction with a similar timeline.

The fourth question asked for a comparison of the exceptions to disclosure in other Canadian jurisdictions. The chart on pages 17 and 18 has a short description of the exception in the far left column and then an indication as to whether a particular jurisdiction has the exception or not.

Finally, section 3.7 of the report contains a comparison of the fees for access to information across Canada, which was provided to our research group by Service Alberta.

The next document is the research briefing, also dated August 25. Research staff were directed to provide an analysis of issues raised that suggest that clarification of provisions of the FOIP Act is required. We looked at 12 different issues, and those were taken from the submissions. Those 12 issues are listed in the table of contents, which is just on the flip side of the cover page. Since we're short on time, I won't address these issues in detail, but I'd be prepared to answer any questions from committee members.

Thank you.

The Chair: Thanks, Stephanie.

Any questions from any of the committee members, starting with Heather?

Mrs. Forsyth: No. I'm fine thanks, Chair.

The Chair: Okay.

Thanks for all the work you guys have done in putting this together. I'm sure we'll have some questions as we go forward on some of the recommendations. This is what we'll be able to use to compare when we're making a recommendation, then, Philip?

Dr. Massolin: Yes. Thank you, Mr. Chair. I am glad you mentioned that because I was going to mention to the committee as well that, of course, these documents may remain pertinent as the committee begins its deliberations a little bit later on.

Thank you.

The Chair: Good. Seeing no more questions, then what we're going to do is take a quick break of eight minutes, a relief break if you will, and then we'll be back for our final two submissions.

[The committee adjourned from 1:52 p.m. to 2:01 p.m.]

The Chair: Welcome back, ladies and gentlemen. It is time for our afternoon presenters.

I'd like to welcome our next speaker, whom we've asked as an expert to come in, Mr. Alec Campbell. At the last meeting there was interest expressed that we find a private-sector expert to appear before the committee to discuss the role of information technology as it relates to the FOIP legislation.

Alec Campbell is the president and principal consultant of Excela Associates Inc. He's been involved in the administration of freedom of information and privacy legislation since 1993. Mr. Campbell is here today as an independent consultant to discuss these matters from his perspective. He has and continues to hold contracts with the government to provide training and expertise. It should be noted that his appearance here today does not necessarily represent the views of Service Alberta or the government of Alberta.

With that, Mr. Campbell, I want to again thank you for making your presentation. Just for the record if you would give your full name and your title. You have 30 minutes to make your presentation because we've invited you; you hadn't made a presentation to us. Then we'll open the floor to questions from the committee after we've introduced ourselves as well.

Excela Associates Inc.

Mr. A. Campbell: Thank you very much, Mr. Chair. My name is Alec Campbell. I'm president and principal consultant with Excela Associates Inc.

Mr. Chair, hon. members, thank you for inviting me to speak to you today. I hope that I can provide some information concerning the emergence of new information technologies, especially their impact on the accessibility and governance of personal information. I'll also raise some related issues that may be of relevance for your review of the FOIP Act. Whether or not they require amendments to the FOIP Act, the issues I raise are significant for the administration of FOIP compliance by public bodies in Alberta. You, of course, will decide whether amendments are appropriate for the issues I address.

Much of my work involves the interface between information technology and privacy. There are many issues associated with the impact of information technology on privacy and access to information. Generally speaking, information technology issues have a greater impact on privacy protection than they do on access to information, although I will mention a few areas in which access may be affected. Because of our time constraints today I'm going to limit my comments to four information technology issues of significance for FOIP administration: extraterritoriality, cloud computing, data consolidation, and security. I'll spend most of my time on cloud computing. Before I touch on that, though, I'll touch on extraterritoriality.

Extraterritoriality isn't just an IT issue, of course, but it is significant for decisions regarding data storage and other aspects of information processing. What we're talking about here is the application of a nation's laws beyond its boundaries.

The USA PATRIOT Act and similar national security legislation in other countries has been a topic of discussion for several years. There have been concerns that personal information about Canadians might be subject to unauthorized access by foreign security services if the information is located on foreign soil or even if it's located on Canadian soil but under the control of organizations subject to foreign laws, subsidiaries of American companies located in Canada, for example. The United States courts are known for their lack of reticence when it comes to the extraterritorial application of United States law.

In response to these concerns amendments were made to the FOIP Act and equivalent legislation in several other jurisdictions in Canada with the intention of making it more difficult for service providers to comply with extraterritorial demands for personal information that's located in Canada but under the control of the service provider. FOIP Act amendments also introduced penalties for public bodies that provided personal information in response to demands from courts without jurisdiction in Alberta.

While these concerns have merit, Canadian national security legislation is largely equivalent to such legislation in many other countries, including the United States. Also, existing treaties would often provide access to personal information about Canadians, in any event. It's therefore not entirely clear whether the extraterritorial application of foreign law significantly increases privacy risk for Albertans. In any event, in my opinion, there's little more that could be done within the FOIP Act itself.

With that, I'll move on to cloud computing, which, with the possible exception of security matters, is probably the most popular topic of discussion today concerning privacy and information technology. This is because cloud computing creates a new paradigm for the custody and control of user data, including personal information, a paradigm that shifts the nexus of control from the client to the service provider. At the same time it offers economies and operational advantages that make it hard to resist for individual and enterprise users alike.

Before I go further, we need to be clear about what we're discussing. The term "cloud computing" refers to computing services and applications in which both the application and the related data storage reside in remote locations and are accessed via Internet connections. The application is online and so are the data. Consequently, the application and data may be located anywhere in the world with an Internet connection. Both data and application are often geographically far removed from the user. This gives rise to a number of factors affecting privacy protection, some of them obvious and some not so obvious.

The first factor is legal jurisdiction. In a cloud computing environment the legal jurisdiction of the service provider is often different from the legal jurisdiction of the user. In Alberta this is almost always the case since few cloud computing services are hosted in Alberta. From a FOIP perspective this means that the service provider is not subject to FOIP or to other provincial legislation such as the HIA or PIPA even though the public user is. If a public body contracts with Google to provide its e-mail services, as some have done, both the e-mail application and the content of e-mails are hosted outside Alberta. In fact, they're hosted outside Canada.

The risk here is that the legislation of the hosting jurisdiction may not require a standard of privacy equivalent to that required by FOIP. This could diminish the level of privacy protection the public body can offer, possibly to below FOIP compliance thresholds. This makes the contractual relationship between the public body and the cloud service provider extremely important, but usually cloud service providers require the use of standard contracts drafted in their own jurisdictions. When that jurisdiction is in the United States, the privacy standards reflected in the contract are often far below the privacy standards required by FOIP. I'll speak to contractual issues a little more later on.

The larger problem is actually more mundane. It is quite simply that it's difficult to know what legal standards apply to the protection of personal information when it's located in jurisdictions outside Alberta. Canadian privacy legislation is fairly consistent, and most privacy practitioners have few concerns with personal information being located in other Canadian jurisdictions. Once personal information leaves Canada, though, it may be subject to quite different privacy standards or, indeed, to none at all.

It's therefore incumbent on any public body that considers storing personal information outside Alberta, especially outside Canada, to know what privacy and security standards will apply to that information. That's often harder than it sounds. It's also incumbent on any such body to contractually bind service providers to a standard of privacy equivalent to that provided in Alberta. For reasons I've already mentioned, that's also more difficult than it may sound, and I'll speak to it a little more later.

2:10

The second factor associated with cloud computing is what I call geographic dispersion. It's related to the previous factor, but it has its own implications. By geographic dispersion I mean that in addition to data being geographically removed from the user, the data may be geographically dispersed among various physical locations, indeed various countries in some cases. Cloud computing service providers are able to locate their data, any user data, anywhere they wish. They're unconstrained by the geographic location of the user, and indeed they are unconstrained by their own geographic location as well. Furthermore, though, one user's data need not be located in just one place. Even a single file can be split among different servers in different physical locations as a result of load-balancing algorithms and other factors.

One example, a personal example here. A couple of years ago I was looking at online backup solutions for my company. I found one that was at the right price point and seemed to have the features I required. I was almost ready to subscribe to it until I found out that the service used servers in several different countries, 16 of them, to be exact, and that any one user's data could be spread among any or all of those servers. That actually could be an advantage from a security point of view, at least from an antihacking point of view, because it would make unauthorized access more difficult. You'd have to access all of the servers to get access to any of the single files that were spread across them.

But the problem was that it also made it impossible for me to tell my clients exactly where their data was. I had no control over the legislation affecting my backup data since new servers were being added in new jurisdictions all the time and others were being shut down for various reasons. As a result, I had to look elsewhere for my backup solution. I couldn't provide adequate notice to my clients related to the location of their personal information.

In addition to complicating issues of legal jurisdiction, the geographic dispersion of data can potentially create problems for some FOIP access requests. Under some circumstances – and I'm not suggesting that this would occur that often, but it is a possibility – it may be difficult for public bodies to thoroughly search their records if those records are housed in the cloud, especially if such searches require the use of search tools not provided by the cloud service provider. Cloud service providers often have proprietary software which is an integral part of their services, and because your data are located on their servers, it sometimes is accessible to the end user only through the software provided by the service provider. If you need to search the data in a way that isn't supported by that search tool, by the tools that the service provider provides, that could be a problem in some circumstances for general access requests.

There's another issue, too, and that is that if data are spread among multiple servers in multiple locations, you have multiple points of failure. From a security perspective, for example, a power outage in any one of those servers could prevent access to the data. That's not unique to cloud computing, of course, but it is a factor.

That leads us into the third cloud computing factor, which is security. A couple of years ago a blogger made the following statement about cloud computing, which rings pretty true for me. He said: a well-configured cloud computing architecture is a hacker's worst nightmare; conversely, a poorly configured cloud computing architecture is a hacker's best dream. What he's getting at is that cloud computing services are not necessarily problematic from a security perspective. In many cases, in fact, they are superior to the security provided by equivalent locally hosted applications. This is because cloud service providers typically require large data centres

for large volumes of user data. Such data centres are normally better secured than computing environments in smaller organizations.

On the other hand, though, such large agglomerations of data are big targets. They are very attractive to hackers, criminal organizations, and others who may seek unauthorized access. The volume of personal information in large data centres can have considerable black market commercial value. Large data centres also tend to have relatively large numbers of technicians, increasing the risk of unauthorized access by insiders. Furthermore, privacy or security breaches often have much larger implications when they involve data centres than when they involve small, locally installed servers.

Another factor to consider is data persistence. Basically, what I mean by data persistence is the difficulty in deleting data. With cloud service providers it can be hard to get rid of your data if you want to. This is a big privacy factor with certain kinds of cloud computing services in particular such as social networking sites like Facebook, which are a form of cloud computing. Users may find it difficult or even impossible to delete their data from the servers. Even if they're successful, there's no guarantee that the data haven't been copied or replicated elsewhere on the Internet. For example, some Facebook applications maintain their own databases of Facebook user data, and those databases may not synchronize deletions with Facebook's own servers.

This isn't an issue with all cloud computing applications. It usually only applies to those that are intended to make user data available to a larger public. Corporate cloud computing environments usually include data management features that reduce or eliminate this risk for corporate data. Nevertheless, public bodies considering the use of cloud computing services must ensure that all their data can be permanently and irretrievably deleted from the service provider's servers on demand or when the services are terminated. I would consider a service provider's unwillingness or inability to provide ironclad guarantees in this regard to be a deal breaker in every case.

That leads into a little more discussion around contractual controls. All of the factors I've mentioned so far mean that when FOIP public bodies consider the use of cloud computing services, contractual matters are all important. Because of the issues raised above, it's critical that the contract between the public body and the service provider impose conditions equivalent to those imposed by FOIP on the public body. Even then there are always potential problems associated with the fact that the service provider is subject to different laws than the FOIP public body. Since a contract rarely trumps legislation, if there's a conflict between the FOIP standards reflected in the contract and the legislation in place in the service provider's jurisdiction, the legislation will usually prevail.

I noted earlier that most cloud service providers strongly prefer to use their standard contracts rather than custom contracts for individual clients. In some cases they may completely refuse to enter into custom contracts. In other cases there may be a willingness to modify certain provisions of the contract or to consider custom schedules, additional schedules to the contract, such as a privacy schedule for larger clients, but unfortunately small organizations and individual users will usually be out of luck.

This is a major consideration for public bodies considering the use of cloud computing services. Public bodies, especially government of Alberta departments, are accustomed to drafting their own contracts with service providers. When dealing with cloud computing service providers, though, they may face the same kind of situation they often face when dealing with major chartered banks; namely, that the standard service provider contract is a take-it-or-leave-it deal. They are not prepared to open those contracts. That can be a problem because the standard cloud computing service contract rarely provides sufficient provisions to ensure that the service provider meets a standard of access and privacy equivalent to that required of the public body under the FOIP Act.

How, then, do we look at mitigating some of these risks? There are a couple of possible legislative approaches to at least a partial mitigation of some of the risks that I've mentioned associated with cloud computing. First, any public body considering the use of cloud computing services involving personal information could be required to prepare a privacy impact assessment and submit it to the OIPC for review. This would be similar to the section 64 PIA requirement in the Health Information Act except that it would apply in a much more limited set of circumstances. In a moment I'll mention one other circumstance in which mandatory PIAs might also be considered.

2:20

Second, the act could be amended to explicitly require public bodies to contractually ensure that computing services and data storage located outside of Alberta comply with the public body's obligations under the FOIP Act. This obligation exists today, but it's not as explicit as it could be, and it's unclear whether all public bodies realize the full extent of their obligations in a cloud computing environment. However, because of the reticence of service providers to enter into custom contracts, this could reduce the number of service providers available to public bodies.

Having said that, local legislation on where the data are stored, as I've noted earlier, will usually override any contract between the service provider and the public body. There's only so much that public bodies can do contractually where there's a potential for conflict with legislation. In many cases, though, the conflict isn't with legislation; it's with the service provider's own policies and procedures, in which case contractual terms can be of great assistance.

Another issue associated with information technology is data consolidation. This is something I'd like to mention specifically in relation to data consolidation and data sharing initiatives within the government of Alberta. As personal information proliferates across government and as pressures to more efficiently process that information increase, there's some pressure to consolidate stores of personal information and use those consolidated stores to service projects and programs in various departments of government.

While efficient data processing is an admiral goal, great care must be taken to avoid the perception that the government of Alberta is or should be a single public body for data sharing purposes. The FOIP Act was drafted in such a way that departments of government were deliberately defined as separate public bodies. The intent of the drafters was to ensure that the collection, use, and disclosure of personal information by government was subject to strict controls, including controls on the exchange of personal information between departments.

The uncontrolled proliferation of personal information across government would seriously compromise the personal privacy of Albertans. It's incumbent upon the government to ensure that such proliferation doesn't occur. Clear standards are required to govern government of Alberta data sharing initiatives that involve the regular exchange of personal information. Whether this occurs through binding government policy or through legislation is not particularly important in my mind, but it must occur.

Given the potential for widespread proliferation of identifiable personal information across government departments, the privacy risks and implications of data sharing initiatives should be subject to rigorous formal assessment. In my opinion, it would be worthwhile to consider making privacy impact assessments mandatory for

projects or systems involving the regular exchange of identifiable personal information between more than one public body. To be effective, such assessments would have to be subject to review by the commissioner. Although large-scale data sharing initiatives often produce privacy impact assessments for review by the commissioner today, making such assessments mandatory would ensure that they're always undertaken, and that's not the case today.

The last issue I'll mention is security. Security is and always will be a critical issue for FOIP administrators dealing with information technology. I've already mentioned some security factors associated with the cloud computing issue. There are many other security risks that are not uncommon among public bodies, including inadequate access controls, high-risk data storage practices such as the failure to encrypt laptop hard drives, excessive reliance on service providers for security planning, inadequate disaster recovery plans, and so forth. The Auditor General has raised a number of these issues in reports over the last several years. There's no time today to delve into them in any detail, but I'd be remiss if I didn't mention them as significant risk areas for FOIP compliance. In my experience, many of these risks affect smaller public bodies more than large ones, but large public bodies are certainly not immune.

Section 38 of the FOIP Act currently requires that public bodies make reasonable security arrangements against such risks as unauthorized access, collection, use, disclosure, or destruction. This provision imposes a general security obligation, but it provides no direction on how to meet that obligation. I'm not suggesting that the FOIP Act should be prescriptive in security matters. Given the rapid evolution of information technology and the security measures it requires, a prescriptive approach is clearly inappropriate. However, there may be room for some elaboration without becoming prescriptive per se. There's reason to consider this. Especially in smaller public bodies there definitely remains a gap in understanding regarding IT security requirements.

For example, the act could require that in addition to its current language there be physical, administrative, and technical measures implemented to protect the confidentiality, integrity, and accessibility of personal information. This would ensure that public bodies consider all the cells of a security taxonomy, which comprises physical, administrative, and technical measures on one axis and confidentiality, integrity, and accessibility on the other axis. Both such axes reflect common and well-understood categories of security measures. Such wording would help to ensure that public bodies cover the security bases, as it were, without restricting them to any specific set of security measures.

One other consideration is of course the issue of breach notification. As you're well aware, Alberta was the first province to require breach notification under the Personal Information Protection Act. I won't discuss this at any length. I think it suffices to say that if private-sector organizations have obligations in this area, it can be argued pretty convincingly that public-sector organizations should have the same obligations.

In concluding, just by way of summary, I've mentioned three areas in which amendments to the FOIP Act might be beneficial to help address information technology issues. These are mandatory privacy impact assessments under certain circumstances, expanded language concerning security measures, and a breach notification requirement similar to the one in PIPA. I'm not suggesting that the act is severely flawed in any of these areas, but there's always room for improvement.

I'll conclude on that note. I'd be happy to respond to any questions you may have. Thanks again for the opportunity to speak.

The Chair: Thank you very much.

Mr. A. Campbell: Thank you.

The Chair: Mr. Campbell, it looks like you must have timed yourself on the presentation.

Mr. A. Campbell: Yeah, I did, actually.

The Chair: It's my pleasure now to open the floor up to questions from our committee members. I know there were some who'd asked about certain issues and wanted to . . .

Mrs. Forsyth: Mr. Chair, I can't even hear you.

The Chair: I'm sorry. I moved the mike. I was just telling Mr. Campbell that I knew that some of the committee members had asked for an expert in here to answer some of the questions that they had, so now is the opportunity for our committee to ask those questions.

Mrs. Forsyth: I have a question for him if you could put me on the list, please.

The Chair: You can start right off.

Mrs. Forsyth: Thank you, Mr. Chair. Thank you, Mr. Campbell. I enjoyed your presentation. I just want to maybe get some clarification on this cloud computing that you were talking about so that I understand it. What's happening now is we have a lot of businesses that are having people doing solicitation; i.e., they're calling from India, et cetera. Are you saying that if those calls are generated from India or something, their privacy legislation is different than what ours would be and we're subject to all sorts of openness in the privacy legislation in places like that?

Mr. A. Campbell: Well, in some places they may be. India has just passed privacy legislation, and I am not familiar with it at all. But that is the essential risk: that in certain locations to the extent that they're collecting or storing personal information, that information may be subject to different privacy standards than exist under FOIP in Alberta. To the extent that a public body is unable to delegate privacy protection to a service provider, that becomes an issue for the public body because it has to ensure that the standards to which it is obligated under the FOIP Act can be replicated by its service provider regardless of where they're located.

Mrs. Forsyth: If I may, Chair.

The Chair: Yes. Please go ahead.

Mrs. Forsyth: I guess I'm trying to follow through with this. For example, can my personal privacy information be sold to – say they're doing solicitation from India – someone else so that they can call me? This hearkens to, like, telemarketers, et cetera. I sometimes wonder how the heck they get your information.

2:30

Mr. A. Campbell: Well, first off, I think you're speaking more of private-sector situations than public-sector ones. Certainly, in the private sector that can happen if there aren't adequate contractual controls over the subsequent distribution or dissemination of personal information, and if there are no legislative controls in existence in the jurisdiction in which the information is being held, there is a risk, then, that your personal information might end up somewhere you wouldn't expect it to end up. To the extent that

public bodies may consider – India may be an extreme example. In most cases the cloud computing services we're talking about are located in the United States or, to a lesser extent, in Europe, but they may have servers in India, so data may still be located there as well.

Mrs. Forsyth: Thank you so much.

The Chair: Thank you.

Ms Blakeman: Well, that was an excellent presentation. I'm really glad the committee asked you to come in. It's exactly the kind of context that I was looking for to help understand. I'm really discouraged right now, actually, because I think sometimes we're fooling around with the small stuff while the big stuff just stomps us.

Okay. Cloud computing. Let me back up. The Ontario Privacy Commissioner is out campaigning right now for a new system called privacy first or something.

Mr. A. Campbell: Privacy by design.

Ms Blakeman: Thank you. Privacy by design. I was struck with that, but in light of what you're telling us, how could we take ourselves back a step and set ourselves up better to protect our citizens? Is it a matter at this point that we would just have to give up participating in certain services or certain sectors that are out there in the world right now? In other words, are we already too late in how we organize ourselves? For example, data storage. I mean, if we said, "Okay, that's it; nobody that is going to have off-Alberta-soil data storage is going to get any of our government or public body business," would we be able to function?

Mr. A. Campbell: You probably could function because cloud computing is very recent. As an effective commercial product it's probably only about five years old. Before that most data was hosted locally or at least with local service providers: Telus, that sort of thing, service farms that were located fairly nearby. I think what's different now is the emergence of large-scale cloud service providers, which can offer very substantial economies, price reductions to public bodies and other organizations. It becomes an issue of balancing cost and operational efficiencies against the standards imposed by legislation, including the FOIP Act but not exclusively the FOIP Act.

As far as what we do about it, the key is in the contract. I think that if there is anything that would assist, it would be to find ways to encourage cloud service providers to be willing to adopt some provisions that they might not otherwise adopt related to FOIP responsibilities around the protection of personal information. So in a number of cases, not dealing with cloud computing but dealing with other contractual relationships, public bodies have added privacy schedules to their contracts. Basically, they either tack on a schedule to the back of the contract or they embed provisions in the contract itself which replicate the requirements of the FOIP Act and ensure that the contract then imposes those requirements on the service provider.

Where you can do that, that's quite an effective approach. The problem arises when the service provider won't consider that kind of contractual amendment. At that point the public body has no choice but to decide whether or not it's going to absorb the risks and go ahead with the contract or not.

Ms Blakeman: But I would argue that given that the government is the only one that's in a position to form that contract or not, it is the government's responsibility to say, "Well, then we're not going to sign it if you will not sign privacy provisions or add a rider," as you say. But how much does that damage our global competitiveness as an economic body?

Mr. A. Campbell: Well, I don't know that that's always going to be the case. It's really a matter of assessing the risk associated with a particular service as applied to a particular set of personal information. The volume of information you're dealing with, its sensitivity, all kinds of factors come into play in the decision, and that's why I'm suggesting that formal, well-conducted privacy impact assessments are critical in these decisions. In some cases it may be that relatively minor amendments or even none at all are adequate. In other cases they won't be. But you need to do a thorough assessment to determine that in each case, I think. It's a due diligence exercise, basically.

Ms Blakeman: Could I get one more supplemental in? Is there a long list?

The Chair: We have quite a list.

Ms Blakeman: Oh, okay. Put me on the end, please.

The Chair: I certainly will.

Ms Notley: Mine, I guess, sort of follows to some extent on what we were just discussing. I might have missed the point here, but I also don't sort of get where the solution lies in this information that you're providing to us because even where you do negotiate the contract, you're still then subject to whatever the extraterritorial laws are.

Mr. A. Campbell: Where there is a potential conflict with legislation, yes.

Ms Notley: Right.

Mr. A. Campbell: But, you know, that's not always the case. In many cases it's just a matter of the service provider having inadequate security measures, for example. There's no conflict with legislation.

Ms Notley: Right. Okay. I thought I had heard you say that you could negotiate our standards into a contract but that if our standards didn't exist in the legislation in the country where the information resides, then our contract might be ineffective.

Mr. A. Campbell: No, I wouldn't quite put it that way. If FOIP standards are negotiated into a contract and there's a direct conflict with legislation in the jurisdiction in which the data are held, then the legislation is likely to trump the contract. That most often arises in one of two circumstances, either where there's some kind of civil litigation that demands the information that's being held or where security services demand it. That's where I was saying that may be a factor. Especially where the security services are involved, there are often other ways for them to get the information anyway. But where those two kinds of things don't arise, where it's just a matter of ensuring that the service provider provide a level of service equivalent to what the public body would want to provide, the contract can be an effective means of doing that.

Ms Notley: What are you proposing is the best mechanism in terms of the work that we're doing on this legislation to deal with these risks?

Mr. A. Campbell: I don't think there's too much that can be done in terms of the legislation itself around contracts unless you're prepared to limit the choice of cloud computing service providers for public bodies. If you're prepared to do that, you could impose requirements that explicitly subject public bodies to the obligation to ensure that their contracts reflect their FOIP obligations.

I think more realistic is a requirement either in legislation or in binding government policy that all potential contracts with cloud service providers not located in Alberta be subject to privacy impact assessments and that those privacy impact assessments be reviewed by the commissioner, as I say, similar to the requirements in the HIA. That way at least you're doing a solid risk assessment in each case.

Ms Notley: Okay.

2:40

The Chair: Thanks, Ms Notley.

Mr. Vandermeer, followed by Mr. Olson.

Mr. Vandermeer: Yeah. My questions were also along the same lines, so you pretty much answered them. I guess what we have to do as a government is just make sure that our contracts are very sound. I think you've answered that question.

Mr. Olson: Thank you very much for the information. It's been really enlightening and a little bit disturbing, too. It makes me realize how old I am because I can remember as a young lawyer studying conflict of laws, which was my least favourite subject – it has to do with, you know, what laws apply in the case of contracts and any number of other things – and I realize how much the world has changed in the last, dare I say, 35 years.

It does make me wonder about whether or not there are any international convention or treaty obligations, those types of things, that might give us a little bit of comfort. If we know that another jurisdiction has signed on to some sort of treaty obligation or convention, that would at least assist with enforcing what's there. I mean, I can counsel lots of clients on contractual issues, where even a contract with one of the parties in Saskatchewan I would say: how are you going to enforce it? It's going to be a lot more complicated enforcing it if you have to go outside of Alberta. I can only imagine how much more complicated it can get dealing with a host of other jurisdictions. It's fine to say that you've got it in a contract, but enforcing it is completely another matter. If you've got, you know, some understanding with those other jurisdictions that they will enforce the contractual obligations that have been made, at least we have something. Are you aware of anything like that?

Mr. A. Campbell: Well, unfortunately, the United States, as you probably know, has no overarching privacy or data protection regime, although there are privacy requirements embedded in certain sector-specific legislation, health care for example. The European Union, though, has a pretty solid set of data protection requirements, and personally I wouldn't be too concerned about hosting personal information in most European Union countries, although I don't profess to be an expert in their privacy legislation. The United States is more difficult.

Australia and New Zealand don't currently host cloud computing services very much, but their legislation is, you know, reasonably equivalent to ours. Same in Hong Kong.

I wish I knew more about India's new legislation because that is, clearly, a very important country for the kind of issues that we're talking about. India hosts a lot of remote computing services, but unfortunately I simply can't speak to their legislation right now.

In terms of international conventions or treaties, though, there's nothing overarching that I'm aware of.

Mr. Olson: Okay. Thank you.

The Chair: Thank you.

Dave Quest, followed by Dr. Raj Sherman.

Mr. Quest: Thank you, Mr. Chair. This has been very enlightening, for sure. You mentioned – and I'd maybe refer this to our legal people later – in section 38 "reasonable security arrangements." In your opinion that is not sufficient.

Mr. A. Campbell: Well, as I said in my presentation, it certainly places the obligation on the public body to ensure that they have adequate security in place. I think, though, it might be helpful for some public bodies, at least, to have a little more direction on what reasonable security arrangements would typically entail. That's where I'm suggesting the use of these common categories of security measures that you will frequently see in security-related documentation. If the legislation were to require that security measures include measures in each of the nine categories that would be created by that three-by-three table, we would have gone a much, much longer distance in ensuring that potential threats were adequately covered off, but we would not have gone so far as to tell public bodies what measures they had to take to cover off those risks.

Mr. Quest: If I can just have a quick supplemental, Mr. Chair. Breach notification requirement: is this common in other jurisdictions? Even if it is or isn't, who gets notified: us and/or the person?

Mr. A. Campbell: In the case of the PIPA provisions the commissioner gets notified, and then the commissioner determines whether or not notification needs to go to individuals who might be affected as well. That doesn't prevent the organization involved from directly notifying individuals, but they don't have to do that. What they have to do is report to the commissioner where they believe that a significant breach of privacy has occurred.

Other jurisdictions. I think it's about 40 of the 50 states in the U.S. that now have breach notification legislation. They don't have commissioners, so it usually requires public notice, notice to any affected individuals. In Europe there is some emerging discussion around breach notification, but I'm not aware of specific provisions. Marylin might be able to help me there, but I'm not sure. Elsewhere in Canada currently Alberta is the only jurisdiction with breach notification, but it appears that it probably will be included in future amendments to the federal legislation.

Mr. Quest: Thank you.

The Chair: Thanks, Mr. Quest.

Dr. Sherman, followed by Ms Pastoor.

Dr. Sherman: Thank you, Mr. Chair. Mr. Campbell, thank you so much for your presentation. As I sat here, I was just daydreaming that I was in a time warp. I used to be a computer geek 30 some-odd years ago on the Apple II Plus computers, where you had to learn all the languages. Never in my wildest dreams would I have thought we'd be discussing these issues today and that technology would have progressed to this point, which leads me to believe that 30 years from now my children will probably have the same concerns that I'm having today.

Just personally – I think I mentioned this before – my information was taken from a dentist's office. There was a privacy breach there. My Visa card was used all over the world in a matter of a few hours. They cancelled my Visa. I think my computer got broken into, hacked by somebody from China. Then my car got broken into two weeks ago. I think the computer hacking was worse than the car getting broken into.

Mr. A. Campbell: Probably.

Dr. Sherman: We discussed one of the most significant pieces of health care legislation recently, amendments to the Health Information Act, and health care information and data and how we use technology are going to significantly improve how we deliver health care. However, the privacy of your personal medical information and protection of that privacy are of utmost importance in the success of the health record. As legislators and as people who are responsible, who in the world does this the best? Who has the best legislation, the best policy, the best systems, and the best protection systems? How should data be stored and protected, and what are the future risks that you see?

Mr. A. Campbell: Well, in answer to your first question, in my opinion Canada has the best protection in existence right now. There are, as I said, other jurisdictions that have similar legislation, notably Australia and New Zealand, but other than that, there are significant gaps, in my personal opinion, in the legislation of virtually every other country. I think we have the most comprehensive privacy regime out there today.

In terms of your third question, I spoke for half an hour on some of the issues and risks that we see, and I think we just have to continue to ensure that due diligence is undertaken when we consider new approaches to the management of personal information, whether it's for health care or for any other purpose.

I'm sorry; I've forgotten your second question.

2:50

Dr. Sherman: How should the data be stored and protected? Who actually physically protects health data the best right now?

Mr. A. Campbell: I think most of the major electronic health record systems are fairly effective in terms of how they protect the data in the data store, so their actual databases are pretty well protected. That's not typically where the risk most often lies. The risk lies with the users and ensuring that the right users have access to the right data but only to the right data and that they know what their responsibilities are in terms of protecting that data.

That said, there are some things that could be done better. In my opinion, data encryption is not widespread enough today. I think there's quite a bit that could be done to improve access control through encrypted data, particularly for mobile devices. I know the commissioner has said frequently that the minimum acceptable security measure for portable data is encryption. There are still many public bodies who are not using encryption for portable data.

Dr. Sherman: Thank you.

The Chair: Thanks, Dr. Sherman.

Ms Pastoor: Thank you very much, Mr. Campbell, for that presentation. The language that you used probably went over my head because I'm not even close to being a computer geek, but the message and the concept, certainly, I think we've been aware of for many years. I guess the point is that if an 11-year-old can hack into the Pentagon – hello? – what chance do the rest of us have?

My concern, like Dr. Sherman's, is also on the health care records. It, quite frankly, scares the hell out of me when I think of the use or misuse that people could have when they get their hands on that kind of information. I'd like a comment on if you think it would be helpful or if it would control if we had a harmonization of the privacy legislation between Alberta's PIPA, the federal Personal Information Protection and Electronic Documents Act, and also Alberta's Health Information Act, if there was some sort of – I don't know – a collation between all of these, if there was that harmonization, if that would help at all in terms of, particularly, protecting health. A lot of these do overlap. Some of them sort of say the same things. It's public-private because, clearly, we are going to have to worry about private health records. As more and more private deliverers come onside, they are going to have a tremendous amount of information that I believe should be protected by a public body.

Mr. A. Campbell: Well, we could easily use up the rest of the day and more on those issues, and to tell you the truth, I didn't really come prepared to talk about HIA issues very much. The only thing I would say in response is that the different pieces of legislation are geared to the protection of privacy in different sets of circumstances. For example, in the private sector privacy is all about consent. It's all about you saying: what's going to happen with my data? If you don't like what a given company does with it, you can usually go to another one. In the public sector that's not the case. In the public sector it's all about legislative authority because often the data collection is mandatory in some sense of the word, and even if it isn't mandatory, you know, there's only one place you can go for the particular service.

In health care it's different yet because in health care there's a strong requirement for the free flow of personal information between health care providers to ensure that the services provided are the best possible. In each of those sets of circumstances you tend to arrive at slightly different kinds of privacy rules, and I'm not sure that it would be possible or even, really, desirable to attempt a complete harmonization of those rules.

I think, though, that the principles behind the privacy legislation across Canada, including all three of our privacy acts – FOIP, PIPA, and HIA – are pretty consistent. If you look at what are known as the fair information practices, which came out of an OECD document on data protection in 1980, all of our legislation is vested in those principles to some degree, so at that level there is a certain degree of harmony.

Ms Pastoor: Thank you.

The Chair: Thanks, Ms Pastoor.

Now Mr. Vandermeer and, if we have time, Ms Blakeman.

Mr. Vandermeer: Thank you. We always talk about value-added here in Alberta, that we don't want to just ship our raw bitumen to the States and then refine it there. What if we were to say: if you want to store Albertans' data, you have to store it here in Alberta? Do we have companies that have the capacity to do that here?

Mr. A. Campbell: The answer to the second question is yes. In terms of data storage certainly there is that capacity in Alberta. When we're dealing with cloud computing, though, in particular, we're also talking about the application. The applications that are of greatest interest to many enterprises today are not hosted in Alberta, so there's some trade-off there. Certainly, organizations

like Telus, for example, have large, very secure server farms, and those are located in Alberta. There was government policy at one point that restricted the location of data for the government of Alberta, government of Alberta owned data as it were, to either Alberta or somewhere else in Canada, that discouraged the location of data outside of the country, certainly, and to a lesser extent outside of the province. While I'm not sure if that policy itself is still active, that is still the position of many government departments. They will avoid locating data outside of Canada where they can.

Mr. Vandermeer: Thanks.

The Chair: Thank you, Mr. Vandermeer.

That hour went by extremely quickly. On behalf of our committee I'll make one observation. This is the least informed person when it comes to technology compared to my colleagues here. When I watch that blond gal on *Criminal Minds* who can hack in and get all kinds of information, if I think that's anywhere closer to reality than my knowledge is, I'm afraid for the future. I really am.

Thank you very much, Mr. Campbell. It was a great presentation, with lots of good information exchanged. We appreciate the work you did in putting everything together to give us good answers and good information.

Mr. A. Campbell: Thanks for the opportunity. All the best.

The Chair: Thank you very much.

Our next presenter is right on schedule, and I will now give him an opportunity to take a chair. We haven't forgotten about you, Mrs. Forsyth.

Mrs. Forsyth: Okay, Barry. Thanks.

The Chair: We're now going to call on Mr. Paul Pellis, Deputy Minister of Service Alberta.

Mr. Pellis: Good afternoon, everyone. How is everybody doing today?

The Chair: Very good. Fresh from Thunder Bay.

Mr. Pellis: Actually, Ohio.

The Chair: Ohio. Okay. As with the previous one, Mr. Pellis, you've got 30 minutes for your presentation, and then we're going to open the floor for questions. For the record your name, your title. I don't know if Ms Blakeman wants to introduce herself to you.

Ms Blakeman: I just had a question before we start. Was your information that you're about to present made available to us on the website, and if not, do you have copies today?

Mr. Pellis: No on both counts, but I will absolutely make that available to you. I'll do that through the chair?

The Chair: You betcha. To the committee clerk would be just fine.

Mr. Pellis: To the committee clerk. Okay. Everybody behind me is taking good notes?

The Chair: They are.

Mr. Pellis: That's great.

The Chair: We understood that you were here to answer questions because you've got quite a familiarity with it, and your department is actually in control of freedom of information.

3:00

Mr. Pellis: That's what I'm told, Mr. Chairman.

The Chair: Thank you. Well, we look forward to the presentation.

Service Alberta

Mr. Pellis: First of all, Paul Pellis, Deputy Minister of Service Alberta. I've been with the department now for five years. I'm attending the meeting today to provide information and answer questions about the relationship between the FOIP Act and information technology developments, contracting, and information sharing.

Before I get into some specific topics that this committee has raised, I wanted to take a moment to talk about the role of Service Alberta as it relates to the FOIP Act. Simply put, Service Alberta is responsible for setting policy and guidelines for government regarding the freedom of information and the protection of privacy. The onus is on each public body to ensure compliance, and the Privacy Commissioner is generally responsible for monitoring how the FOIP Act is administered. The FOIP Act itself is designed to be technology neutral. It reflects a set of principles which in theory can be broadly applied to any kind of information or records.

As we're all aware, technology is a rapidly developing field. All governments are striving to utilize new technology developments as quickly as possible, particularly in areas where we can better service the public and reduce our costs. With the dynamics of changing technology it's important that legislation be principle based with a strong focus on standards.

The next thing I want to talk a bit about is cloud computing. One of the innovations that's challenging public bodies today is the concept of cloud computing. Traditionally computer applications and electronic document storage have resided on a user's workstation or secure computer network. To prepare a document in Microsoft Word, Word must first be installed on a user's computer. Once a user has completed working on a document, it is stored on a user's computer or on a secure network.

Cloud computing is a different approach. In one version of cloud computing file storage, e-mail, and other computing applications are managed by third-party providers. Applications do not reside on an individual's laptop or computer. Applications are accessed via the Internet or on servers operated by a third-party provider. For example, as an alternative to buying Microsoft Office software, Google currently offers free online applications for word processing, spreadsheets, and presentations. The use of online computer applications is often referred to computing in the cloud.

You may wonder: why would a public body consider using this type of cloud computing? The most significant advantage is decreased costs. In some cases services are free. In others services are billed on a consumption or subscription basis. The use of this open type of cloud computing can eliminate the need for software licences, upgrades, and other significant costs. Services can be accessed anywhere, at any time, and from any computer.

Recently, as many of you are aware, the University of Alberta decided to adopt Google's Gmail for all staff and student mail. To address access and privacy concerns, the university conducted a privacy impact assessment, which was reviewed by the Information and Privacy Commissioner's office.

Unless appropriate mechanisms are in place to restrict access to information residing in the cloud, it should be assumed that all stored data may be accessible by the cloud service provider and visible to outsiders, even if only by accident. The GOA ensures that