HOUSE OF COMMONS
CHAMBRE DES COMMUNES
CANADA

Standing Committee on Access to Information, Privacy and Ethics

ETHI • NUMBER 025 • 1st SESSION • 42nd PARLIAMENT

EVIDENCE

Thursday, September 29, 2016

Chair

Mr. Blaine Calkins

Standing Committee on Access to Information, Privacy and Ethics

Thursday, September 29, 2016

● (1100)

[*English*]

The Chair (Mr. Blaine Calkins (Red Deer—Lacombe, CPC)): Good morning, colleagues. This is the 25th meeting of our committee and we're still studying the Privacy Act.

We are pleased to have with us today Mr. David Fraser, a partner at McInnes Cooper and no stranger to this committee; and Michael Geist, Canada research chair in Internet and e-commerce law, and professor of law here at the University of Ottawa.

Gentlemen, neither one of you is unfamiliar with this process. The process of our committee allows about 10 minutes for introductory remarks from each witness. We'll start with that and then we'll proceed to rounds of questions until everyone is satisfied. I think we have the full two hours with just two witnesses, so that gives us plenty of opportunity.

I'll start with you, Mr. Fraser, if you're ready to go.

Mr. David Fraser (Partner, McInnes Cooper, As an Individual): Thank you very much.

Thank you for the opportunity to speak about this statute, which is one of the most important statutes we have to regulate the interaction between individual citizens and their government.

The Privacy Act was great for the 1980s, but much has changed since then. This committee has heard a lot about changes in technology, but I think one overarching consideration is changes in people's expectations. We have seen developed, in a number of different jurisdictions across Canada, much more modern privacy laws. We have the Personal Information Protection and Electronic Documents Act, which regulates the private sector and is based on fair information practices. I believe this committee has also heard a lot about the new ATIPPA statute in Newfoundland. You had the benefit of speaking to the committee responsible for the report that led to its complete revamp.

One thing worth noting, when you are looking at this statute compared with other more modern privacy statutes, is that consent generally does not work in the government context. Individual citizens don't choose, for example, the government with which they deal, compared with choosing which bank they go to, and things like that.

One thing I want to emphasize, first and foremost, is that I have had the opportunity to review and actually contribute to the Canadian Bar Association's submissions over the years. Although I am speaking in my own capacity, I generally agree with everything that's in there. Also, I am in general agreement with what has been noted and asked for in the Privacy Commissioner's submissions to this committee over the course of a number of years. There are a couple of things I would like to specifically highlight that I think are important to look at.

One is what could be a basic technical fix, which is to remove the requirement that personal information be recorded in order to be subject to the statute. Information that is just stated orally, that is handed over.... The statute can be interpreted such that the disclosure of information orally is not captured within the statute, and that is a significant gap.

I also think that there should be a provision in the statute to clarify that the work product of public servants should not be considered to be personal information of those public servants. This statute should work hand in hand with the Access to Information Act to encourage transparency of government operations. Unwarranted calls for privacy standing up in the face of government transparency are problematic and something that can be quite easily addressed.

The rest of my recommendations or suggestions would probably be lumped in under three different categories: accountability, transparency, and overall making the statute effective.

Under the accountability banner, I would think that we need more clarity, as citizens, about how government manages the personal information of its citizens. We have the personal information banks and info source systems, which I don't think are entirely effective. There needs to be more proactive disclosure to citizens about how their information is used, who is responsible for it, and which government department is using it.

There should also be a necessity test, which is something this committee has heard about, with respect to the collection of personal information. The government institution should collect only information that is necessary for its functioning activities.

I think there should also be an element of personal accountability within the statute, which is missing. Many more modern privacy laws, particularly health privacy laws but also others across the country, have an offence provision that if an individual or even an institution, unlawfully and usually with knowledge, is in violation of the statute, they can be charged under that. We have seen a large number of privacy breaches across the country related to individuals just browsing through large databases for their own entertainment, and charges being brought against those individuals in various provinces. I think that's something that should be introduced into the Privacy Act.

Under the heading of transparency, fair information practices are generally based on notice and consent. As I said, consent isn't something that generally works in the public sector context, but I do think that there needs to be more proactive communication to citizens about what the information is going to be used for in order to justify its collection. Other jurisdictions regularly include privacy notices on the forms that they require citizens to complete, letting them know and setting their expectations with respect to why the information is necessary, how it is going to be used, who is going to be the custodian of that information, and how they can get access to it and have it corrected, if necessary, to exercise their other rights under the statute.

Also in connection with transparency, I think that the Privacy Act should specifically give the commissioner an education mandate, but along with that it should also give the commissioner the ability to publish reports of findings of investigations under the Privacy Act.

● (1105)

Currently the commissioner publishes such findings for private sector investigations, but we need more guidance. Transparency about what the government is doing with respect to personal information would be significantly served if there were such an obligation, or at least the mandate and the ability for the commissioner to report findings. In the annual report that the commissioner issues each year, there are summaries of some notable cases, but I think we would all benefit from understanding what government departments are doing with people's personal information. Having that information out there, particularly if it's found that the government department has not acted properly, would serve a significant education mandate for all government departments, but also for citizens generally.

I do think we need to have breach notification if there's a breach of security safeguards, similar to what was added to PIPEDA in the Digital Privacy Act, an obligation on the part of the government institution to notify both the Privacy Commissioner and notify affected individuals if a proper threshold has been met. I think the one in the Digital Privacy Act is a reasonable one.

Then ultimately, there's making it effective. I'm not a fan of order-making powers. I think the ombuds model works, but I have come around to see the wisdom of the Newfoundland hybrid model, where if a government department is not going to follow a recommendation with respect to any obligation under the Privacy Act—collection, use, disclosure, or other safeguards—the department should have to stand up in front of a court and justify it and explain why it doesn't have to. In effect, that puts the onus on the government department, and we would end up with a body of case law that would be more clear. That could be by an expedited application process, which is already the procedure under PIPEDA, so that these don't turn into significant, huge federal cases.

Those are the highlights of my recommendations for the statute. It is really outdated, really antiquated, and I don't think it accords with the evolved expectations of individuals about how their information is going to be collected, used, and disclosed. We shouldn't tolerate a quasi-constitutional statute that's at least two generations out of date.

Thank you very much.

The Chair: Thank you, Mr. Fraser.

Mr. Geist, you have up to 10 minutes, please.

Dr. Michael Geist (Canada Research Chair in Internet and E-commerce Law and Professor of Law, University of Ottawa, As an Individual): Thank you.

Good morning, everyone. As you heard, my name is Michael Geist. I am a law professor at the University of Ottawa, where I hold the Canada research chair in Internet and e-commerce law.

My areas of specialty are digital policy, intellectual property, and privacy. I served for many years on the Privacy Commissioner of Canada's external advisory board, and I have been privileged to appear before many committees on privacy issues, including things such as PIPEDA, Bill S-4, Bill C-13, the Privacy Act, and this committee's earlier review a number of years ago on social media and privacy.

I appear today though, as always, in a personal capacity representing only my own views. As you know, there is a sense of déjà vu when it comes to Privacy Act reviews. We have had many studies and successive federal privacy commissioners who have tried to sound the alarm on legislation that is viewed, as you just heard, as outdated and inadequate. I think that Canadians rightly expect that the privacy rules that govern the collection, use, and disclosure of information by and within the federal government will meet the highest standards, and for decades we have failed to meet that standard.

I would like to quickly touch on some Privacy Act concerns, but with your indulgence I'll talk a bit about some of the other broader privacy law environment issues in Canada that I think are really directly related to the Privacy Act.

First though, on the Privacy Act—and this is going to sound familiar as I have flagged some of the same issues that David did—I think the Privacy Commissioner of Canada has provided this committee with many very good recommendations, and I endorse the submission. As you know, most of those recommendations are not new. Successive commissioners have asked for largely the same changes, and successive governments of all parties have failed to act.

I want to highlight four issues in particular with respect to the current law, and as I say, David has flagged some of them already. The first is education and the ability to respond. The failure to engage in meaningful Privacy Act reform may be attributable, at least in part, to the lack of public awareness of the law and its importance. I think the Privacy Commissioner plays an important role in educating the public, and has done so on PIPEDA and broader privacy issues. The Privacy Act really needs a similar mandate for public education and research. Moreover—and you just heard this—the notion of limited reporting through an annual report, I think, reflects a bygone era. In our current 24-hour, social-media-driven news cycle, restrictions on the ability to disseminate information, particularly information that can touch on the privacy of millions of Canadians, can't be permitted to remain outside of the public eye and left for annual reports when they are tabled. Where the commissioner deems doing so to be in the public interest, the office must surely have the power to disclose in a timely manner.

I also think we need to think about strengthening protections. As you've heard, the Privacy Act falls woefully short of meeting the standards of a modern privacy act. Indeed, at a time when government is expected to be a model, it instead requires far less of itself than it does of the private sector. A key reform, in my view, is the principle of limiting collection, a hallmark of private sector privacy law. The government should similarly be subject to collecting only that information that is strictly necessary for its programs and activities.

I'd also flag, as David did, breach disclosure, which has been commonplace in the private sector privacy world, and it has long been clear that similar disclosure requirements are needed within the Privacy Act. The Treasury Board guidelines are a start, but legal rules, in my view, are essential. In fact, the need for reform is even stronger given the absence of clear security standards within the act. Provisions that establish such standards and mandate disclosure in the event of a breach are crucial to establishing an appropriate level of accountability and ensuring that Canadians can guard against potential identity theft and other harms.

The final issue is privacy impact assessments. As you all know, privacy touches us in many ways, and it similarly is implicated in many pieces of legislation. I recall that during the last session of Parliament, the Privacy Commissioner regularly appeared before committees to provide a privacy perspective on many different pieces of legislation. This approach of coming in after the legislation has been drafted at the committee, I think, runs the risk of rendering privacy as little more than just an afterthought. It's more appropriate to conduct a privacy impact assessment before legislation is tabled, or, at a minimum, at least before it's implemented.

Those are some of the issues on the Privacy Act side, but as I said, I wanted to talk about three bigger picture issues that I think are some of the moving parts in the federal privacy world.

● (1110)

The first has to do with Bill C-51's information-sharing provisions. I realize the government is currently consulting on national security policy, and there's, as you know, a particular emphasis on Bill C-51. From my perspective, one of the biggest problems was the information-sharing provisions. The privacy-related concerns stem from an act within the act in Bill C-51's Security of Canada Information Sharing Act. As you may know, the sharing of information went far beyond information related to terrorist activity.

It permits information sharing across government for an incredibly wide range of purposes, most of which have little to do with terrorism. The previous government tried to justify the provisions on the grounds that Canadians would support sharing of information for national security purposes, but the law now allows sharing for reasons that I think would surprise and disturb many Canadians, given how broadly those provisions can be interpreted.

Further, the scope of sharing is very broad, covering 17 government institutions, many of which are only tangentially related, if at all, to national security. The background paper on the national security consultation raises the issue, but in my view appears to largely defend the status quo, raising only the possibility, it seems to me, of tinkering with some clarifying language. If we don't address the information-sharing issue, I fear that many of the potential Privacy Act improvements will be undermined. I think this requires a wholesale re-examination of information sharing within government and the safeguards that are there to prevent misuse.

Second, I want to talk about transparency and reporting from a slightly different perspective. As many of you may know, in recent years, there have been stunning revelations about requests and disclosure of personal information of millions of Canadians, millions of requests, the majority of which are without court oversight or warrant, which I think points to a real weakness within Canada's privacy laws. Most Canadians have no awareness of these disclosures and have been shocked to learn how frequently they are used.

Recent emphasis has been on private sector transparency reporting. Large Internet companies such as Google and Twitter have released transparency reports, and they have been joined by some of Canada's leading communications companies such as Rogers and Telus. There are still some holdouts, notably Bell, but we have a better picture of requests and disclosures than we did before. However, these reports represent just one side of the picture. Public awareness of requests and disclosures would be far more informed if government also released transparency reports. These need not implicate active investigations, but there is little reason for government to not be subject to the same expectations on transparency as we expect of the private sector. Indeed, the Liberal Party focused on transparency in its election platform. Improvements to access to information are absolutely critical, but transparency is about more than just opening the doors to requests for information. Proactive disclosure of requests for Canadians' information should be part of the same equation.

Third and finally, I want to talk briefly about government-mandated interception capabilities and decryption. The public safety consultation that I referenced, which was launched earlier this month, has been largely characterized as a C-51 consultation, but it's much more. The return of lawful access issues threatens to scrap the 2014 lawful access compromise, and I think raises some really serious privacy concerns.

For instance, the consultation implies that “lack of consistent and reliable technical intercept capability on domestic telecommunication networks” represents a risk to law enforcement investigations. Yet left unsaid is that the prior proposed solutions in the form of government-mandated interception capabilities for telecommunications companies were rejected due to the enormous cost, inconsistent implementation, and likely ineffectiveness of standards that would exempt many smaller providers. Creating government-mandated interception capabilities for all providers represents an enormous privacy risk that I think runs roughshod over both PIPEDA and the Privacy Act.

Further, the consultation places another controversial policy issue on the table, noting that encryption technologies are “vital to cybersecurity, e-commerce, data and intellectual property protection, and the commercial interests of the communications industry”, but lamenting that some of those same technologies can be used by criminals and terrorists.

Given its widespread use and commercial importance, few countries have imposed decryption requirements. This year's controversy involving access to data on an Apple iPhone that was owned by the San Bernardino, California, shooter revived debate over access to encrypted communications. The consultation asks Canadians to comment on circumstances under which law enforcement should be permitted to compel decryption. A move toward compelling decryption, in my view, would place more than just our privacy at risk. It would also place our innovation strategy and personal security in the balance.

● (1115)

In conclusion, fixing the Privacy Act is long overdue. There is little mystery about what needs to be done. Indeed, there have been numerous studies and a steady stream of privacy commissioners who have identified the problems and called for reform. What has been missing is not a lack of information, but rather, with all respect, a lack of political will to hold government to the same standard that it holds others.

I look forward to your questions.

The Chair: Thank you very much, Mr. Geist. We have some very interesting testimony here that we can ask questions about.

We'll move to the seven-minute round for the first four questioners.

Mr. Lightbound, please.

[*Translation*]

Mr. Joël Lightbound (Louis-Hébert, Lib.): Thank you, Mr. Chair.

Since I'll be speaking in French, I'll ask the witnesses to put in their earpieces.

Thank you, gentlemen, for being here today.

Mr. Geist, I have been following your work for a number of years. I want to tell you that the way you have been holding the government responsible and accountable is very patriotic. Thank you for doing so for all the issues you have addressed.

My first question concerns the exceptions in the Privacy Act.

For example, section 2 indicates that government agencies can share information with each other. Bill C-51 states that we must comply with the Privacy Act. The act says that information can be shared between institutions if the regulations of other federal acts are respected.

Aren't we squaring the circle somewhat, in the sense that the protections found in the Privacy Act are becoming obsolete? I want your opinion on the matter. How should we address the exceptions or authorizations for sharing information found in the Privacy Act?

● (1120)

[*English*]

Dr. Michael Geist: I could start if you like, and I'd start first by thanking you for those really kind words. It's almost as if my mother were on the committee. Thanks so much. That's really kind.

This represents one of the most challenging issues that we face. Notwithstanding the fact, as I indicated, that I feel like there has been a lack of political will to address what's clearly a thorny issue, part of the challenge is how you strike some balance in these issues.

When I think of some of the exceptions that we find in the act and what we saw coming out of Bill C-51, I think there is a broad desire to recognize that in a data-driven world there is value in that data and we want government to be smarter and to act smarter and be able to use some of that information. Part of it stems from thinking about safeguards that can be adopted by government that are similar to what we find within the private sector, the de-identification of data in many instances, so that the value in the data may not come from specific individuals but rather comes from the information in aggregate and looking to government to adopt some of those same kinds of practices.

Where that's not possible though we have to start thinking about strengthening some of the reporting mechanisms from within government and creating stronger oversight mechanisms within government, recognizing that there are going to be instances in which sharing is important, and sometimes on an emergent basis, has to happen. But what we haven't had, and this was touched on by both of us off the top, is a framework of accountability that allows for the public to better understand when that's happening to allow independent officers to conduct more effective reviews and then ensure that the public is aware that's happening when it does indeed happen.

[*Translation*]

Mr. Joël Lightbound: My second question is for the two witnesses.

You did not discuss it in your presentations, but certain authorities, for example, in Canadian airports, have collected metadata on Canadians to obtain a very clear picture of an individual's virtual itinerary.

Do you think the Privacy Act would be the right place to define metadata? Should we focus on that angle or should we instead find the definition in the National Defence Act or in other legislation?

[*English*]

Mr. David Fraser: I'm happy to provide my thoughts on that.

The Privacy Act is well placed to consider metadata as a concept. The definition of personal information in the statute, if it's fixed in order to deal with the recorded or not recorded thing, is information about an individual. Metadata is information about an individual whether you're talking about metadata or the actual content, that's all information about an identifiable individual and it's all personal information.

With respect to specific uses or collections, authorities to collect information, particularly for national security purposes, it does make sense that it would be located in a statute related to national security.

My thinking on that topic is that for years I have been hearing principally from law enforcement people suggesting that metadata is like dust; it's nothing. In fact, metadata can be everything when it comes to information about people's biographical core. Certainly your travel itinerary doesn't tell you who you spoke with at the end of your journey but it tells you where you went and how long you were gone for and all that sort of information. I do think it needs to be managed as personal information. To suggest that it's something completely apart from personal information trivializes it, and I think it's actually a bit deceptive.

Dr. Michael Geist: I would largely echo David's comments.

I can recall appearing before a couple of House and Senate committees on Bill C-13, the lawful access bill, and much of the discussion for many of the witnesses was to try to emphasize the import of metadata. It's refreshing to have the issue raised right off the top and to have a recognition of the privacy import of that information.

I think the privacy community and the technical community, both of which have come forward on these issues, have consistently tried to argue that what we need is to take metadata far more seriously as a privacy issue. That has been largely missing. Frankly, we were met with largely dismissive responses and the law enforcement perspective that this is little more than dust and the sense that, somehow, lower thresholds were appropriate.

Yet when you take a look at what that metadata can ultimately reveal, as authorities in the United States have sometimes said.... I think Stewart Baker, the former general counsel of the NSA, has said, “We kill people based on metadata”.

The value of that information and the potential import of that information is huge, so I don't think it's a question of where it appears. I think it's actually essential that we address it as equivalent to some of the most sensitive privacy information that we potentially have both in our Privacy Act and in other legislative instruments where that same data is touched on.

● (1125)

[*Translation*]

Mr. Joël Lightbound: Mr. Geist, my next question is for you.

Which model should inspire us at the international level? I know, for example, that the Germans have quite strong privacy laws.

Is there a particular model you think could inspire our committee when we review the Privacy Act?

[*English*]

Dr. Michael Geist: I could start by saying that, interestingly, Canada itself, on the private sector side, for example, has been viewed as a model. That's not to say that PIPEDA is perfect. It is not.

Mr. Joël Lightbound: That's our next item of business.

Dr. Michael Geist: There is definitely room for improvement there, but if you take a look at some of the competing perspectives on privacy, you see that the European perspective tends to adopt more of a human-rights-oriented approach, and the U.S. perspective tends to be somewhat more commercially oriented. The Canadian compromise, I think, is generally viewed as a good one.

What makes the Canadian approach an effective one, I think, is that it's based on international privacy principles, principles that have been updated over time. If we want to look to what kind of standard or what sort of example we need, I don't think we have to look far. Those kinds of standards, the kinds that I think you've heard about pretty consistently now, are not reflected in the Privacy Act today. The starting point is to do a mapping, in a sense, of what is seen as the standard and to look for ways to ensure the Canadian law measures up.

The Chair: That takes us pretty close to eight minutes, Mr. Lightbound.

Mr. Fraser, if you have something else to add to that, I'm sure there will be an opportunity.

We now move to Mr. Jeneroux, please, for seven minutes.

Mr. Matt Jeneroux (Edmonton Riverbend, CPC): Thank you very much.

Thank you, Mr. Lightbound, for officially tipping your hand as to where we're headed next, although I'm certain you would still appreciate the debate on this side of the table for—

Mr. Joël Lightbound: I should have said that it could be our next item.

Mr. Matt Jeneroux: Yes, it could be. I appreciate that.

Thanks to both of you for coming today. I appreciate your taking time out of your day to be here before committee.

Mr. Fraser, I didn't write down your words quickly enough, but did you say that you prefer the hybrid model as your approach? Can you explain in a bit more detail why that's the best model as the order-making model so that we have it on the record?

Mr. David Fraser: Certainly. Not having any teeth in the legislation I think is ultimately problematic. Forcing the individual concerned to be the one who goes to court and has the onus of proving to the judge that somehow their rights have been infringed I think places too much of a burden on the individual. Also, when you simply look at the economics between the two—the government and an individual—that's a pretty daunting prospect for an individual.

There is probably greater opportunity when the commissioner doesn't have the ability to compel the person to do something, but does have a lot of authority in terms of the ability to sit down and discuss it. I've certainly seen this in the private sector. It's a much less confrontational approach. The commissioner would have the ability to work with the public body in order to exercise moral suasion to convince them that “this is it and that ultimately this is the recommendation”. Then, if the government institution decides that they're not going to follow that recommendation, they should be the ones to stand up in front of a judge and say that they're not legally required to do this. You can clearly have a difference of opinion.

To me, it's as much not wanting to change the character of the interaction between the office and the individual, or the office and the institution, and wanting to make sure that the onus is properly on the right party, and also that the burden ultimately is on the right party. I do think it also allows a greater degree.... If the commissioner has an education mandate and an advocacy mandate and all these other sorts of things, you don't want to turn the commissioner into essentially a tribunal as well. You want to separate that as well. The commissioner makes a recommendation. If the institution decides not to follow it, the onus could be on them to justify that.

● (1130)

Mr. Matt Jeneroux: Mr. Geist, do you have any thoughts on the order-making hybrid model?

Dr. Michael Geist: I do. Most of my thoughts, I must admit, are within the private sector context. I haven't been privileged enough to see what takes place within those internal discussions between the Privacy Commissioner and a government department. I do believe—and I guess I would differ with my colleague—that order-making power is necessary, certainly in a private sector context.

I say that for at least a couple of reasons. I think the experience we've had over the last number of years demonstrates that real penalties matter. The Conservative government was sometimes criticized for its position on some privacy legislation, but one area in which it enacted very tough rules—and I think we've seen some of the effect of that—was the anti-spam legislation. There are debates about the legislation to be sure, but what I think is indisputable is that the legislation had the effect of getting businesses' attention in a way that legislation without teeth doesn't. We see that difference.

I would also say that we now have enough experience with companies being quite willing to disregard the Privacy Commissioner's views that I think a tougher position is needed. A classic example would involve Bell—it comes up again, I suppose—in the decision involving relevant targeted advertising. There has been a long process of investigation, with input from many Canadians. I think they got more complaints over that particular issue, when it started getting some attention, than over virtually any other. The commissioner has made a finding, and Bell's initial position is “well, that's nice; that's your view; we disagree”.

It's not clear to me, given the import we place and the responsibility we place on the Privacy Commissioner, how companies can adopt that position and basically say, “See you in court, and let's litigate this for a few years before we decide what will take place”. Bell ultimately backed down, but I think the presence of order-making power would have changed that dynamic considerably.

Mr. Matt Jeneroux: That's Interesting.

To switch gears a bit to talk about technology and the constantly changing technology we're seeing, the Privacy Act, as I believe both of you indicated, hasn't been changed since 1983. However, there are a number of policies within government that are maybe a bit more adept and nimble to cover some of these things. I'm curious to hear your thoughts on how much you see being covered under the act versus under a policy within a department that would be specific to emerging technologies.

Mr. Geist, you mentioned that you were here for the PIPEDA social media review. I'd like to hear from both of you about how much of this we should consider including in the act.

Dr. Michael Geist: I can start by saying it's always a challenge to keep pace with technology, and we all, I think, recognize that the legislative process moves at a different speed than technology does. That's, I think, a given. Filling in where technology has raced ahead and there is a need for an urgent response, I think, at times will make sense. But at the same time, I do think you have to get your foundational pieces of legislation right, and that means updating them on a pretty regular basis.

In fact, it was the Conservative government that on at least a couple of areas that are really my bread and butter in a sense—copyright and privacy—made a strong point of saying that they wanted to build in mandatory reviews to ensure that the legislation would stay up to date in a rapidly changing environment. A copyright review will take place next year. PIPEDA was one of the first to try to do the same thing by saying we'd have a mandatory review every five years. I don't think that's been well respected, quite frankly.

I think you have to get the foundation right. While there is a role for supplementing legislation where issues emerge, this legislation scarcely covers the VCR era. We're going back a long way if we're trying to think about the technology that was relevant at the time the legislation first came in versus the technology of the world we live in today. Notwithstanding some of the efforts to address some of those issues through directives and the like, what we fundamentally need is to re-establish what the baseline happens to be.

The Chair: Thank you very much. We're at a little over seven minutes.

Mr. Blaikie, go ahead for seven minutes, please.

Mr. Daniel Blaikie (Elmwood—Transcona, NDP): Thank you very much.

Mr. Fraser, in your presentation you talked briefly about the notion of the work product of civil servants not being able to be interpreted as private data of any kind. Could you just flesh that out a bit more or give a particular example or instance? Can you talk a bit more about how that works presently, and what needs to be fixed?

● (1135)

Mr. David Fraser: Certainly.

The Access to Information Act mandates transparency, but it has exceptions for unreasonable invasions of privacy, and it has some clarification language about what the thresholds are. Of course, it uses the same definition of "personal information" as in the Privacy Act.

One thing that has been developed in the private sector is a recognition that there's a work product exception, and that a document you produce in the course of your work as part of your job is not your personal information. It's not about you, so you can't use a privacy argument pulled out of thin air to try to stand in the way of disclosing that. George Radwanski was, I think, the first commissioner to bring this up. He had to almost make it up within the statute.

In regard to information about where a particular public servant was posted at a particular time, for example, sometimes I've heard, "That's a privacy issue. We can't let you know that." Information about their role, their position, and even about their salary is information about government operations that should be transparent.

Information about a deputy minister's calendar, other than doctors' appointments obviously, can be usefully used in order to keep government on their toes and keep them accountable. Too often I've heard, "We can't do that because of the privacy law." I think there needs to be some real clarification, not just in policy but in the statute, to make it clear that is not an excuse to stand in the way of government accountability.

Mr. Daniel Blaikie: One of the other themes you both mentioned today that has come up in previous testimony is mandatory breach reporting, and also, having penalties for breaches. One of the tensions there, of course, is worrying that an institution, for example, might cover up a breach they're supposed to be reporting because they fear the penalties. We had one witness talk about, not having consequence-free reporting of a breach, but maybe changing the scale of consequence in cases where certain kinds of measures had been taken, including encryption and so on.

Do either of you want to speak to that interplay between reporting and penalty, and give your thoughts on what a successful regime might look like?

Mr. David Fraser: In the amendments put into the private sector law, PIPEDA, by the Digital Privacy Act, there is a threshold that represents a real risk of significant harm. Part of that is a statement of principles, but if the information is encrypted and nobody can get access to it reasonably, that significantly lowers the risk of significant harm, so it might not even trigger the notification threshold. I think that there does need to be some flexibility. You don't want to be too prescriptive in that sort of thing.

Importantly, Parliament introduced new offences into the private sector legislation, through the Digital Privacy Act, related to not reporting those breaches. If you do not report one of those, you can in fact be convicted of an offence. I'm not sure that necessarily works in the public service per se. I think it's worth looking at. There should be an assumption that the government will follow the law if the law says you shall report it.

I would, in fact, be in favour of lowering the threshold for reporting to the Privacy Commissioner so that the Privacy Commissioner can provide knowledgeable, informed input on whether or not the breach actually represents a real risk of significant harm, and the commissioner should himself be able to notify the individuals at the institution's expense if the institution refuses to.

Dr. Michael Geist: David hits on a good point. In a breach-disclosure regime you do need thresholds. People who are ardently pro-privacy are going to say that if we adopt the lowest of thresholds so that just about everything is going to get reported, not only are there going to be significant costs associated with that to organizations, but the reporting and disclosure system is largely going to turn into noise from the perspective of individuals. The whole goal here is to get their attention and to allow them to deal with the issue.

If what we have are notices going out on a daily basis because we have an incredibly low threshold, the news value of those stories will be largely eliminated because it will just be another day, and the individuals will increasingly just ignore them despite the fact that we have a lot of expense.

I think David is right. The issue is how to ensure that the right instances, those where there is a real risk, get reported back to the people who are affected, and at the same time remove the potential reticence of organizations, both in the private and the public sector, to at least do the initial report so that we can engage in a meaningful consideration of the risk.

Lowering the threshold and ensuring that you have a body that will keep it confidential and is well trusted like the Privacy Commissioner offers a pretty nice balancing system that allows for external consideration of the risks involved and also ensures that where there is a real need to know for those who are affected, they are notified.

● (1140)

Mr. Daniel Blaikie: On the slightly different topic of transparency reporting, I just want to ask, is that something the infrastructure already exists for? Is that something that is just a matter of publicly reporting something that departments would be doing anyway? If not, what kind of infrastructure do you need? How big of an organizational change is it to implement regular transparency reporting?

Dr. Michael Geist: I'll start by saying I think it depends a little bit on who's doing the reporting. Let's start with law enforcement and some of those law enforcement requests. We know that it took many years to even get to the point where law enforcement was tracking some of this kind of information. They did so largely because the demands for easier access to this information were being met with questions, “How often are you accessing this? Give us some actual data.” It turned out there was very little data to be had.

We now have some data, but I think it's still fair to say that there are many law enforcement branches that are either not fully collecting all this information or are using a bit of a haphazard mechanism. If there were requirements to disclose, there would also be requirements to more systematically collect.

It seems to me that, in fact, it's in the interests of not just of the public having access to information but of those organizations too. We have some of those same entities now saying they want to have easier access to this information, notwithstanding the 2014 legislative compromise and the Spencer decision from the Supreme Court of Canada. I think they've got an onus to at least begin to provide more data on what's actually been happening that moves away from the odd anecdote here or there.

At the moment, we're heavily reliant on what we can learn from either the Internet companies or some of the telecom companies without, as I mentioned, uniformity. I think we need to look at the other side of the coin as well in creating obligations for the systematic collection and then disclosure, and I think aggregating that information is very important.

The Chair: Thank you, Mr. Blaikie.

We now move to our last questioner in the seven-minute round, Mr. Erskine-Smith.

Mr. Nathaniel Erskine-Smith (Beaches—East York, Lib.): Thank you very much.

My first question relates to information sharing. The Privacy Act governs information sharing. The Privacy Commissioner has recommended written information-sharing agreements between departments.

Mr. Geist, you suggested we need a wholesale re-examination of information sharing with specific reference to the new act. Can we deal with the problems that you identified with respect to the new act within the Privacy Act? Are there ways that we should be changing the Privacy Act to deal with information sharing in a more substantive way, or should this committee be, in our future studies, looking at that new information-sharing act and making recommendations for both?

Dr. Michael Geist: Thanks for the question. On that last bit, I think it's not necessarily an either-or issue. I do think there is unquestionably a role for this committee on some of those issues. For example, one of the other issues that I've been spending a lot of time on lately is the Trans-Pacific Partnership, the TPP. As I'm sure you know, there are multiple committees that have been examining the impact of the TPP. Certainly, international trade, but not just international trade. Agriculture and others are taking a look at the implications of that agreement for their ambits.

I think the same is true when we take a look at what's taking place in that part of the national security consultation. I think there are clear implications for a number of other committees, and not just this committee either. For example, it seems to me it's pretty clear the implications of some of the issues that I've talked about have a huge impact, or would have a huge impact, on the communications industry, the industry committee, or ISAT, or whatever we're calling it nowadays. If it doesn't take a look at those issues, then I think we're missing a piece of the pie.

Mr. Nathaniel Erskine-Smith: Other than the Privacy Commissioner's recommendation that there be written information-sharing agreements, is there anything else that we could put into the Privacy Act that would help govern information sharing in a more substantive way?

Mr. David Fraser: I would think that a general statement of principle related to that would have a natural home in the Privacy Act, to say that any formal or informal information-sharing arrangements between a government institution and another government institution or another government.... Federal-provincial information sharing takes place all the time, as it does internationally between CRA and the IRS in the United States. Increasingly, we're seeing that sort of stuff. There should be a decision-making framework on what's in, what's out, what's okay, and what's a consistent use, thinking of why the information was collected in the first place. All of those MOUs should be in one place, on one website, and available to the public to really understand what is in fact going on.

● (1145)

Mr. Nathaniel Erskine-Smith: Perfect.

With respect to remedies and recourse, you touched on them a little bit. There were some questions on this a bit previously. What model would we be looking at? There's PIPEDA, for example, under sections 14 to 16, and there's an application to court and you can seek damages. The last I checked, an illegal strip search was worth $5,000. We're not talking a great deal of money perhaps, but is that the model we'd be looking at, or are there other models we should be looking at as far as judicial recourse and enforcement of remedies go?

Mr. David Fraser: My initial thought is that there is a distinction between going to court to force government to do what it legally is supposed to do and preventing it from doing what it legally is not supposed to do: kind of your classic judicial review, or the implementation of an order to do or not to do something.

When it comes to harm to individuals that has happened in connection with these sorts of things, I would, first of all, want to make sure that there is nothing in the Privacy Act that cuts off that possibility. There is a section in there already that says that no government institution, crown servant, or otherwise, has any liability for any action it takes in good faith under the legislation. That has been used by the federal Department of Justice to say, "We are immune to lawsuits." That was thrown out by the Federal Court of Appeal in a hearing I was involved with in April.

Again, you want to make sure that individuals who are in fact harmed—because we are seeing an increasing recognition in the case law, in the evolution of the common law in Canada and the civil code in Quebec, that privacy harms can be significant.

Mr. Nathaniel Erskine-Smith: Should we statutorily enable such claims? Obviously, the current statute.... There is case law now that is undoing what the government would like to rely upon in the statute. Should we actually enable that through the statute?

Mr. David Fraser: I would be careful about doing that. Other privacy statutes, in the rest of Canada, have provisions that allow individuals to seek damages after it has gone through the Privacy Commissioner process. The courts have generally said that this doesn't actually close the door on the other avenues, but you want to be very careful that it doesn't.

You can see a mechanism.... For example, you mentioned, quite rightly, that the privacy harms are relatively modest when it comes to just general damages, hurt feelings, embarrassment, and things like that. It is seldom worth an individual's effort to hire a lawyer and go to court to recover $5,000's worth of damages.

If you want to enable individual claims on a relatively low threshold in terms of the expense, I think that makes a lot of sense, but if you make it so that it has to go through a complaint to the Privacy Commissioner first, then on, there is no mechanism, for example, in PIPEDA for a kind of a class doing that. One applicant gets to go to the Federal Court in order to get a finding and get damages. You don't want to close the door on that, which would ultimately be a licence to the federal government to commit a huge amount of harm for which it would not be legally responsible.

Mr. Nathaniel Erskine-Smith: With respect to necessity, it is not an idea we have really explored, but I just want to get at this. I am trying to think of an example. I think there is legislation now introduced in the House with respect to collecting information at the border. CBSA is now going to know when folks leave, and we are going to collect data about how many days they have been out of the country, which we haven't been collecting to date in a specific way. Just tracking that data point and sharing it with other government agencies that perhaps want to know, for example, if someone is making a claim to health or to government services, would that fall within the scope? As we think about necessity, would that fall within the scope of proper information sharing? It obviously enables government to do the job that it should be doing, in terms of making sure services are going to the people they should be going to. Is that consistent with the word "necessity?"

Dr. Michael Geist: I'll start with the typical lawyer response. I think it depends.

I can envision a couple of scenarios drawn out of your particular example. I can envision a scenario where, let's say in Ontario, OHIP or the provincial Ministry of Health has reason to believe that an individual has been outside the province or outside the country for an entire year and thus shouldn't qualify for health insurance. There is some evidence to that effect, so as part of its more routine anti-fraud investigations, it looks to find different data points it can collect. One can argue that in those instances it is necessary.

A different situation, though, might well be that there are claims that one way to reduce health care spending at a provincial level is to try to weed out those who aren't eligible who are claiming so that we need to be actively monitoring everybody's movements to try to proactively identify who doesn't qualify and thus remove them from the insurance rolls. That doesn't strike me as a particularly wise thing to do and wouldn't meet the kind of standard that we might want to establish.

● (1150)

The Chair: Thank you very much.

Mr. Fraser, answer briefly if you can, please.

Mr. David Fraser: I was just going to say that there is a continuum. You can always find a second, third, fourth use for information that has been collected. I do think that there needs to be reasonableness put in there, but having transparency about what government is doing, how they are doing it, and for what purpose allows Canadians to actually understand what is happening and to question it if it's problematic.

The Chair: That was a good discussion.

We move now to the five-minute round with Mr. Jeneroux.

Mr. Matt Jeneroux: Thank you.

Getting back to my previous question, Mr. Fraser, we'd love to hear some of your comments—quickly—about blending technology into the act and how much we should consider in the act to keep up with emerging technologies and so forth.

Mr. David Fraser: One of the wonderful things about Canadian laws generally is that they are usually technologically neutral. You don't focus on a technology.

Certainly, technological changes can necessitate a kind of revisiting and updating, which obviously is the case here with the Privacy Act, but I think what has driven the need to update the Privacy Act actually isn't technology. That fed into it, but in fact it was people's differing expectations and understanding of what privacy is, having more control over your personal information and more of a say in those sorts of things, and recognizing that privacy harms can take place.

In 1983, the question was much more 1984-related in terms of "we need to regulate what the government collects because you'll end up with Big Brother". In this day and age, there's just so much information that's collected everywhere, not just in government but elsewhere, that Canadians' expectations of privacy have evolved, and the statute needs to do that.

If the committee is going to suggest wording changes in the statute, for example, I would caution you to avoid dealing with the technology. It's better, I think. PIPEDA is a real model of how you can come up with a privacy statute that's based on principles, bedrock principles that I think most Canadians can get on board with. That's the skeleton on which you put the meat, but you want to make sure that it will in fact stand the test of time. As an additional protection, the five-year reviews are imperative for a statute such as this.

Mr. Matt Jeneroux: That's great.

If I could, I'll get both of you to comment on the recommendation by the Privacy Commissioner to extend the act to the ministers and to the Prime Minister's Office as well. I think you've loosely touched on it, but if you don't mind commenting a bit again, we could have some of that on the record as well.

Dr. Michael Geist: I'm supportive of that recommendation, and supportive of it for the same reason that I'm supportive of some of the shift toward thinking about access to information in a more wholesome manner that captures some of that as well, which I know the government has talked about.

Again, when I think about some of the issues that I have focused on in the past, that divide between ministerial offices and departments is increasingly blurry. That's not to say that the department doesn't function as a department in providing the best advice it can to the minister's office—of course it does—but the decision-making and policy development now occur not just in the department. They quite clearly occur very often in the ministerial offices, so from my perspective, having an understanding of those processes and ensuring that they are subject to the same kind of transparency and openness requirements is important. That means ensuring that the Access to Information Act covers it, but I think it also means that the Privacy Act does as well.

Mr. David Fraser: I would generally agree with that, although I would add that I think there's a difference between the Privacy Act and the Access to Information Act in this. One can understand that you have cabinet confidences and things like that, but there shouldn't be a system that would allow an office within the functioning of government to collect information and use it in a way that otherwise would be completely unlawful. You end up with a complete zone of non-regulation in that particular place. You wouldn't want to, for example, set up a system that would encourage a program to be operated out of a minister's office in order to avoid the functioning of a quasi-constitutional statute.

● (1155)

Mr. Matt Jeneroux: Thanks.

The Vice-Chair (Mr. Joël Lightbound): Thank you.

We'll move now to Mr. Saini.

Mr. Raj Saini (Kitchener Centre, Lib.): Thank you very much to both of you for coming here. It's been quite interesting.

I'm going to ask a similar question in two different forms.

Mr. Geist, I've read some of your writings. You talk about a policy called "opt-in consent", which I found very intriguing.

You brought up the Ministry of Health, so I want to give a bit of background. As pharmacists, one thing we've found is that whenever any patient wanted to sign up for the government drug plan, they first of all had to opt in to give consent and also to provide specific information. To verify their income, they had to give specific consent so the health ministry could talk to CRA to make sure the income was verified, in order for the ministry to determine and discern what deductible group they were going to be in.

Here's my question for you. When we talk about government agencies and government departments, sometimes they may have to talk to people but opt-in consent is not given. You've said that you feel that should be the default approach. How do we strike that balance to make sure the government is still effective and still running efficiently? Could you maybe highlight how we can strike that balance?

Dr. Michael Geist: I'd start by noting that some of my writings around opt-in consent have tended to focus on the private sector side, where we have legislation in PIPEDA that opens the door to both an opt-out and an opt-in system. It seems to me that the opt-in standard is a more effective one from a privacy perspective, and I think leaves individuals with much better knowledge about what they're actually agreeing to and how their information is going to be used.

As Mr. Fraser pointed out off the top, the consent model doesn't map as nicely on the public sector side because there's lots of information that government is going to collect with or without our consent. In a sense, our consent doesn't really matter. There is certain data that you have to have.

Your particular example is a good one though because it takes us into the realm not of collection but rather of use, and raises the prospect of asking if we could establish, or if we should establish systems that more effectively give people some amount of control over their information, not necessarily at the collection level—although even there we could think about what we could do—but more at the use level and at that sharing level.

Are there certain things that we don't need consent for because there is no reason to think about consent? Where we are looking more into opting into certain kinds of programs and it is necessary to have that information to do it, then you can make the argument that, perhaps it's more appropriate to say, if you don't want to avail yourself of that service or that opportunity, that's your choice. But the only way that you can is if you provide the necessary consent.

Mr. David Fraser: I'm in agreement with Professor Geist on that. There are opportunities, particularly if somebody is enrolling in a program, that they don't have to, where it is in fact much more of a voluntary relationship. Mostly your relationship with the government is involuntary, but when it's voluntary, we need to be absolutely clear and transparent. I think we should make efforts to avoid surprises.

Privacy is one of those weird things that really goes to the core of people's emotional well-being. They want the autonomy. They want control of their information. If you tell them that as part of enrolling in this program, there is going to be income verification and it's going to take place a certain way, and the person signs up, they're not going to be surprised and they're not gong to be upset by that. Or they can question whether it's really necessary, and in that way, they get to participate as a much more informed citizen.

Mr. Raj Saini: The second question I have is particularly to you, Mr. Fraser, because you've also written about the fact that the physical location of data is not that important anymore. In your previous brief you highlighted two cases, one on Microsoft and one on eBay.

Based on that, sometimes, as you know, there is going to be data sharing between governments. When we receive data—let's say we have asked for taxes for someone who is living in a different country—we take that data and we have it reposed in CRA, but that data could possibly be shared with other government agencies and departments without that person knowing.

We still have a regime here that's still foundationally sound. It can be improved. I can agree with that. In other countries, that may not be the case. Information could be shared without the person knowing, and their privacy regime may not be as robust as ours. How do we reconcile that?

● (1200)

Mr. David Fraser: I think that one of the themes of my writing and thinking on this topic is that the location of the data is one factor, but it's not the overwhelming *sine qua non* of what the issue is. There are other factors that go into it. The Treasury Board policy related to this topic is in fact a really good and really rational approach to it, which is, if any government department is going to make any decision about the location of data in connection with outsourcing, or anything else like that, location is going to be a factor, but there are other things as well. Who is going to be the service provider? Who are they beholden to? What national ties do they have?

We're starting to see a more nuanced evolution of this as a question, which is in contrast to the situation in Nova Scotia and British Columbia where they have a statute that says thou shalt not allow the personal information outside of the country. You can still hire an American service provider to manage it for you on your own territory, and they—at least according to the U.S. Department of Justice—are as subject to the Patriot Act when they stand in Canada as they are in the United States. Just saying it needs to be here doesn't alleviate all those concerns. We need a nuanced risk analysis understanding.

There's been mention a number of times of privacy impact assessments. I think those are a really great tool that give you the opportunity to look at whatever is going on from a number of different perspectives, a number of different privacy risks, to force you to think about how to mitigate this and if the risk is acceptable depending on the sensitivity of the information, and then to have those reviewed by the commissioner and have those made public so there's transparency into these sorts of decision-making functions.

The Vice-Chair (Mr. Joël Lightbound): Thank you very much.

We're out of time, Mr. Saini, but we'll have plenty of time at the end.

Mr. Jeneroux.

Mr. Matt Jeneroux: Thank you.

You both touched on privacy impact assessments. I would like to get more details on why you think it's necessary that they're enshrined, specifically, into the act, as opposed not to.

Dr. Michael Geist: Unless you establish clear signalling and a prioritization within the act, you end up with what we have had for the last period of time, which is that privacy too often becomes an afterthought on legislation that has a significant privacy impact.

On the legislative side, baking privacy into the process is important, not so much privacy by design, so to speak, as it's sometimes referred to, but rather ensuring that there's a recognition that considering the privacy implications of legislation is essentially part of the legislative-making process.

Further, and this was touched on in David's comments a moment ago, where you're confronted with some of the really challenging issues that the last question raised around location, around transfer to what we might see as low protection jurisdictions, whether for sharing purposes or other transfer purposes, one of the ways to at least begin to think about whether or not this is something we ought to be doing or whether or not there ought be some limitations established is to conduct privacy impact assessments.

The move to enshrine that legislatively has a signalling effect, and it also may have a real world effect in ensuring those kinds of things happen.

Mr. David Fraser: I would echo that.

If Parliament puts that in the Privacy Act, it says that this is, in fact, an absolute priority. If it's left in a Treasury Board policy somewhere, it's at the whim of the government and it could be reversed. If you do not do a privacy impact assessment, and you're legally required to under under the act, you've broken the law, which is more than slightly different from just avoiding a policy, skipping a policy, or a procedural step.

Mr. Matt Jeneroux: Wonderful. That's all I have.

The Chair: Mr. Long.

Mr. Wayne Long (Saint John—Rothesay, Lib.): Thank you, Mr. Chair, and thank you to the witnesses. This is a very interesting discussion.

I want to begin with a blog that you wrote, Mr. Fraser. You said, “You’d better forget the right to be forgotten in Canada”.

I thought that was really interesting. I can give you an example. When I was with the Saint John Sea Dogs, a hockey team, we had an issue with a teddy bear toss. To make a long story short, the teddy bears, potentially, were infested with bedbugs. We had to cancel the teddy bear toss, but for years and years, if you Googled “Wayne Long”, the first thing that came up was bedbugs. Whether I wanted that or not, I couldn't get rid of it.

You're of the view that:

> ...the right to be forgotten cannot be shoehorned into existing privacy law because search engines do not come within the scope of PIPEDA and the activity of indexing newsworthy content online is subject to the journalism exception in PIPEDA. Furthermore, any attempt to compel a search engine to not include particular results—particularly pointing to lawful content—would fall afoul of the freedom of expression right under the Canadian Charter of Rights and Freedoms.

Can you elaborate on that, give me more? Maybe Mr. Geist, you can comment as well.

● (1205)

Mr. David Fraser: It's a very complicated issue. I'm not unsympathetic to people like yourself. I've represented and advised clients. A significant part of my practice is cyber-bullying, helping individuals who've had issues.

You are not alone. I've certainly had people across the table from me crying because their dating lives and other parts of their lives have been impacted by what shows up in search engines.

Mr. Wayne Long: It's a good thing we won the Memorial Cup and I'm in politics, because now that's bumped way down low.

Mr. David Fraser: Excellent. That's a practical strategy for dealing with that issue.

The issue is how to fix that in a legal sort of way, consistent with our Charter of Rights and Freedoms that has section 2(b), and our privacy law that has a journalism exception. We don't think the same way as in Europe where, in fact, privacy takes precedence over freedom of expression. In Canada, you usually have a balance when it comes to charter rights. You have a charter right to freedom of expression. You don't have a charter right to privacy, other than unreasonable search and seizure.

It's a complicated argument, but I don't think that one can find a way in PIPEDA to make that work in the way that people who talk about the right to be forgotten talk about it. In a practical sort of way, most of those search results would be newspapers that were reporting on it.

Mr. Wayne Long: Right.

Mr. David Fraser: You would not be able, in Canada, to get a court order requiring a newspaper to unpublish something that was true. Our body of case law related to freedom of expression, defamation, and other things like that support that entirely. If you can't tell the newspaper not to publish it, not to make it available anymore, should you be able to tell an uninterested third-party search engine to not tell people that it exists?

Mr. Wayne Long: What do you suggest? What do you recommend?

Mr. David Fraser: I'm not sure I have a solution. I have the advantage of getting to stand on the sidelines and point out problems. To the extent that I can contribute to solutions, I'm happy to. The problem is always going to be a threshold one, and I think the problem needs to be addressed by the people who are publishing it, rather than intermediaries who are pointing out that it exists. The analogue is, you wouldn't hold a librarian liable for telling you that down in the basement in the dusty stacks is a newspaper from 20 years ago that has this article. You need to be consistent. It's not the technology that necessitates making the rules. Technology might make new problems surface, but our democratic framework that includes freedom of expression needs to be superimposed over all those decisions.

I think this Parliament did a fantastic thing with Bill C-13. The first part of it related to the non-consensual distribution of intimate images. I've seen first-hand the huge amount of harm that sort of activity causes my clients. I think that is a very helpful addition, and that can be put in the continuum of the right to be forgotten. The Ontario courts have made it possible, just under the common law, for an individual to get a remedy in damages for that horribly harmful behaviour, and that can lead to an injunction to get it taken down.

One can easily say at the extreme end of the continuum that, when you're dealing with horrible revenge porn, whatever you want to call it, it's absolutely deplorable. There's no doubt that laws can work on that, but things like those teddy bears having bedbugs are part of living in a modern world.

Mr. Wayne Long: Mr. Geist.

Dr. Michael Geist: I have a couple of comments. First, I'm not particularly supportive of the right to be forgotten. I have seen it come up in a context. Actually, I sit on the board of CanLII, the Canadian Legal Information Institute, which makes Canada's laws and decisions available online. Those have been available online for a long time. We don't index through Google, although we've had a number of instances where people have captured many of those decisions. They've been made available through Google, and people have found out that a decision from many years earlier is in fact available online.

I must admit I've never been particular sympathetic about the need to remove that information. The need is to address it up front, let's say in the court context, by redacting, say, sensitive family information from court decisions. Once it's published, open-court principles apply. I think the same is largely true in this context.

The one place that I would differ slightly from what David was talking about is over the issue of jurisdiction over search engines, whether we could compel them to do something. In fact that exact issue—not in the exact same context—is before the Supreme Court of Canada in a decision that will be heard in early December, Equustek v. Google, in which the B.C. courts have ordered Google to remove from their search results certain content that a B.C. party alleges violates their intellectual property rights. The B.C. courts have ordered Google to do so, not just for the search results that are made available to Canadians through Google.ca, but rather for the entire world.

● (1210)

Mr. Wayne Long: Okay.

Dr. Michael Geist: So we have Canadian courts saying they can do it. Our Supreme Court of Canada will presumably render its view as to whether or not Canadian courts get to decide for the rest of the world by asserting jurisdiction in that fashion.

Mr. Wayne Long: Okay, thank you.

The Vice-Chair (Mr. Joël Lightbound): Mr. Blaikie, you have the last questions, for up to three minutes.

Then, colleagues, we'll have some time if you want to get on the list.

Mr. Bratina, I see that. Is there anyone else who wants to have a little more time? I'm sure the witnesses will stick around as long as we have intelligent questions to ask them.

Mr. Blaikie.

Mr. Daniel Blaikie: Thank you.

Professor Geist, in earlier remarks you mentioned that you're part of a working group on the implications of the Trans-Pacific Partnership around privacy and digital issues. I was wondering if you want to give us a better idea of some of the issues that are coming up in those studies and the potential implications in terms of whether some of those provisions would be able to.... We know that in some cases deals like that sometimes echo back through government policy and affect what governments feel they're able to do.

Are there any issues where that's a possibility with TPP?

Dr. Michael Geist: There are. It's not so much a working group as it's an issue that I've done a lot of writing on. I appeared before the committee on international trade and was one of the panellists at one of the town halls that the government held on the TPP.

There are some privacy provisions. The TPP has an e-commerce chapter, which is really a first in many ways for a trade agreement of this kind, certainly for Canada. It includes some privacy provisions. In my view, it establishes an incredibly low threshold. It does so largely for the private sector. It calls on TPP countries to establish privacy rules, but in a footnote notes that if companies simply put out privacy policies and then there is an enforcement arm to ensure that those privacy policies are abided by, that is sufficient. That's a nod to the United States, which doesn't have overarching privacy rules.

I suppose the position I've taken on the privacy provisions in the TPP, like many of the digital provisions, is that I thought Canada has a good story to tell and has policies, whether it's on privacy or in a number of other areas, that I think reflect considered long-standing discussions and debate about striking appropriate balances, because there's always a balance to be struck on a lot of these issues. Unlike the United States on a lot of these digital issues, which looks to these trade agreements to try to proactively take their policies and see them reflected in trade agreements so that they'll be reflected in other countries, which has the effect of seeing better laws all around the world but also of ensuring that their companies and others know that if they're compliant locally they can look to the same kinds of regimes elsewhere, I thought the Canadian negotiators were really disappointing in that regard and simply didn't prioritize those kinds of issues. Canadian businesses that seek to comply with Canadian rules under our Canadian system won't see those same kinds of rules reflected elsewhere due to the TPP, which I think is a missed opportunity at a minimum.

Mr. Daniel Blaikie: What does that mean for their competitive advantage if we're signing into a trading bloc and Canadian companies are being held to that higher standard, which is the right standard, but now companies operating in other jurisdictions that have a lower threshold are now able to come in without any added...?

Dr. Michael Geist: Those companies still have to meet Canadian standards if they operate in Canada or are collecting information, let's say in the privacy context, from Canadians. It's not that they get a free pass in that regard. It's that, if we take a look at the U.S. strategy, notwithstanding the claims that people like Donald Trump are making about whether or not the U.S. is a winner or loser on the TPP, the U.S. has long sought to carefully and closely align its commercial interests with its trade policy. They actively discuss with their businesses about where they're headed and they try to ensure that their businesses' priorities and their legal systems are reflected, because they believe there's a competitive advantage in having that reflected in trade agreements.

Canada didn't do that in the TPP. It's one of the reasons why you see some prominent business leaders being highly critical of the agreement. I think, as I say, it's a mistake that ultimately puts us at a bit of a competitive disadvantage.

● (1215)

Mr. Daniel Blaikie: Okay, thank you.

The Chair: All right, good.

Mr. Bratina, please.

Mr. Bob Bratina (Hamilton East—Stoney Creek, Lib.): Thank you.

You mentioned the old technology and the VCRs. I'm old enough to well remember the Nixon tapes. It leads me to ponder who owns what data and how it is collected. For instance, if I had a conversation with the Prime Minister in his office and there happened to be a recording device, could I ever ask in a subsequent argument or discussion to use the contents of that device?

Those are just some general thoughts, but what I'd like to ask you directly is to reflect on Hilary Clinton's emails, and how, in our deliberations, we might ponder similar situations occurring or how we can avoid whatever problems she's going through. You certainly must have pondered her predicament.

Dr. Michael Geist: I think the starting point is to not send your work emails through your own server at home.

It feels a bit more like an access to information issue in many respects. The question of emails has been challenging, because of course we want government, the bureaucracy, and others to adopt efficient means of communication. I have launched the occasional access to information request, and if you ask for all records, you get emails as well. There was a time when those revealed a lot, of course subject to all the various exceptions, and those exceptions also removed a lot. Nevertheless, you could often read between the lines on quite a lot because they revealed a fair amount.

Once certain departments, in my experience, found that people were asking for that data, one of the things that started happening was that people stopped communicating via email and started finding other ways that fell outside of that. Part of the discussion on Clinton has been revelations about her discussions with, I think, Colin Powell, and there has been talk about how you can structure a communication system that falls outside of the act.

I think in some ways we've had some of the same kinds of things take place here with people either engaging in discussions that they ensure don't take place by email—the so-called PIN discussions through BlackBerry—or sometimes even doing direct messaging through Twitter. They are finding mechanisms that may fall outside of that system.

My response is that, by and large, where the discussions fall within the discussions of government and policy and the like, and the act applies, the solution isn't to try to find ways to get around those rules. The solution is to try to ensure that the legislation is sufficiently robust to cover them.

Mr. David Fraser: This is Right to Know week, and in fact there's been a lot of discussion about that particular topic in connection with transparency within government. Part of it is a notion of a duty to document, which I think touches on an important thing that Michael just raised, that government decisions need to be properly documented and they need to be documented in the proper way and in the proper place, which should be on government-managed information systems. I'm a strong believer in keeping your personal emails out of your work inbox and keeping your work emails out of your personal inbox. There should be a divide between them.

Mr. Bob Bratina: In the recommendations that came forward from the commissioner, recommendation 13 suggests that discretion be given to discontinue investigation of complaints in specified circumstances, when they are vexatious and so on. Mr. Drapeau disagreed.

Where do you come in on the commissioner's discretion to not handle so-called vexatious or otherwise frivolous complaints and so on?

Mr. David Fraser: I think it should be possible. I think the commissioner should have the ability, because there are, no doubt, vexatious litigants out there and there are people who abuse the process. You would want to institute it with the appropriate checks and balances and possible judicial review, because cutting somebody off from redress under the Privacy Act is a pretty significant step given its quasi-constitutional status in Canada.

I've seen a lot of abuses of the statute, and certainly I'm sympathetic to a commissioner having to open a file and go through the whole process for something that really, at the end of the day, they know is going to go nowhere. However, I really hesitate to give anybody a tool that cuts somebody off from effective legal redress.

● (1220)

Mr. Bob Bratina: Professor Bennett suggested limiting these complaints to perhaps three. He said these types of frivolous, vexatious complaints often come in reams of questions. Are there any remedies? Does that sound like a fair way of approaching this problem?

Mr. David Fraser: I think that's probably too blunt an instrument since every case stands on its own. The courts have developed a meaningful test for what is a vexatious litigant. I don't think you need to recreate anything out of whole cloth. There's something already there. It always does take into account the nuances and the circumstances. I think that's probably appropriate.

I would not want to see an enormous amount of resources wasted for nothing, but again as I said, I'm concerned about cutting people off from effective redress.

The Chair: Colleagues, with your indulgence, I'd like to ask a few questions. Is that all right?

Mr. Geist and Mr. Fraser, I'd like to follow up on something that Mr. Erskine-Smith was addressing. This is with regard to secondary or tertiary uses of information. Let's say legislation is put before the House and is passed for the capture of information for a specific purpose. It's used, for example, for somebody exiting the country. It's used to determine whether or not somebody qualifies for health care benefits, because we do have rules and laws pertaining to that. However, now all of a sudden it becomes much easier for, say, Stats Canada to capture how many people are leaving the country and the travel locations of certain Canadians, or it becomes something that maybe CSIS or other organizations might want to have access to.

What things should we as a committee be recommending to the government insofar as primary purposes for capturing information? How well should that be laid out? What kind of detail and legislative rigour need to be put around making sure that people's privacy is protected and that information is only used for what it was initially intended?

Dr. Michael Geist: I'll start by saying that I think we do need to flesh out some of those issues. I think it's an important one, and I'm glad we've had the opportunity to talk about it.

For some of the kinds of information we're talking about, consistent with some of the remarks David made at the very outset, there isn't a consent issue there. Some of it will get collected. That's simply a fact. There is this spectrum, and I think David referred to it, where there are certain kinds of uses that don't raise particular concerns or perhaps are sufficiently important that we would say, yes, you ought to be able to use it in those circumstances, provided it's appropriately documented and there are the appropriate kinds of oversight.

There are also, even implicit in your question, departments whose interest in the information may not be in the personal information, per se, but rather in the aggregated data. On the private sector side, the way organizations often deal with information is to say they don't really care about the individual, but they do care about that aggregated data. There may be aggregated data where we can say that as long as we're able to separate that out and find mechanisms to remove the personal side from it so that it's used in an aggregated fashion, there's actually a lot of value, and government can act in a smarter fashion.

It's probably a somewhat unsatisfying answer to again come back to “it depends”, but what we need are rules that recognize that there may be times when those secondary uses can happen without implicating the personal side of personal information. There may be secondary uses that it's kind of nice to have. In those circumstances, appropriate levels of consent seem to me to be the order of the day. There may be instances when it's essential to have access to that information. We need a sufficiently robust oversight and reporting system that doesn't necessarily stop the sharing in those circumstances, because we recognize the import of the sharing. Rather, we need a system that ensures that there is not misuse and that there is appropriate transparency associated with that activity.

Mr. David Fraser: I'm in general agreement. There is a recognition in most privacy statutes, and even in the public sector, that you collect information for a purpose. It has to be authorized by law or it has to be reasonably connected to an operating program of the public body. That information can be used for that purpose or for a use compatible with that purpose. There is a body of case law, within the commissioners at least, that talks about that: what is that compatibility?

I think part of it has to do with a direct connection. Is there a direct connection between tracking somebody's status leaving and determining whether there's a likelihood that somebody's going abroad to engage in terrorist activities? Those are both national security contexts. You see those as being relatively adjacent and possibly justifiable. CBSA sharing that information with CSIS might make sense in the circumstances, but that should be under an information-sharing MOU that should be available for public scrutiny. If they want to share it with the tourism department, for example, I can't imagine that being so directly connected.

The nature of the information needs to be taken into account. How sensitive is it, and really, on balance, is it worth doing this? You also have to be mindful of Canadians' expectations. You can always think that any little bit of data the government has can probably be useful someplace else. You need to think about whether it's reasonable in the circumstances that it would be used in that other place, particularly when you look across the very broad diversity of government institutions. The Department of Health provides primary health care to the aboriginal people of Canada. That's a huge amount of very sensitive information about individuals that should never find itself over in Stats Canada, other than in the aggregate, or that shouldn't find itself over in CSIS just because the government of the day has decided to knock down the walls between the departments.

● (1225)

The Chair: That's interesting. In the time I've spent in Parliament, I have had opportunities—as I'm sure many of my fellow members have—where a constituent comes to us and it's evident that an inappropriate sharing of information between government departments has happened. The constituents in some cases feel as if the government is out to get them. A third party might look at it and say it was just a mistake, but we did talk a little bit earlier about having some teeth in legislation and some accountability.

I'm wondering if you could flesh out any of this, because I believe that there have been several instances where constituents have come through my door about this. There have been several others where I believe it was simply an honest mistake made by workers in the government. But I have reason to believe that there are constituents I represent that seem to have found themselves on...I don't know if there's a list, but let's just say that people from different departments talk to each other, meet over coffee, move around between various departments. If a particularly difficult citizen is causing them grief, I'm sure these things get discussed. I don't know if there are instances where it's provable, simply because one person standing up alone against the government is very difficult.

I think Brian Mulroney said that one of the biggest things we can do as members of Parliament is to make sure that the government hasn't the ability to crush a person if it wants to.

What kinds of safeguards should we be discussing when it comes to the Privacy Act, when it comes to access to information—which I know is beyond the scope of this study—to ensure that individual Canadians have the right to defend themselves against the information that the government can, if it chooses, maliciously use against them?

Mr. David Fraser: That is a very big question, and it raises a number of different aspects that I think are relevant for this study. One thing that I think is very important is the ability of a member of Parliament to help an individual constituent. That's already in the Privacy Act. Maybe it's worth making that a little bit more robust. The next step is to make sure that it is as easy as possible for an individual to get meaningful redress from the office of the Privacy Commissioner of Canada, making sure that the commissioner has the ability to get all the relevant information to find out what went on.

I mentioned earlier the possible offences related to somebody intentionally flouting their legal obligations under the statute in order to hold people accountable for actual mischief, not just administrative mistakes, which can happen in a large organization. One example that you have given provides a number of opportunities to think about the different layers and different points in time of what a good system will look like. Ultimately, if that person is actually harmed, is there a mechanism by which they can get effective redress? Somebody can be kicked off a benefits program for a year, and that can have a significant impact on their income, things like that. They need a way to make things right, because now, way more than in 1983, we recognize that harms to privacy are real harms.

● (1230)

The Chair: I know Mr. Erskine-Smith wants to get in here, but I have one other question and I'm simply seeking your opinion.

In my own capacity just as a regular Canadian, my expectation is that when I do business with the private sector or the government, my privacy should be protected and considered. I expect that my rights to have access to this should be almost seamless. I'm sure both of you will be back when we review PIPEDA. In our deliberations, we know that the Privacy Act has to work at the same time that access to information needs to be implemented.

What considerations should we be looking at when making our recommendations to the government, assuming legislation is coming forward, finally, with no prejudice? What considerations should we be taking into account when making it easy for Canadians to have basically the same expectations, whether they're dealing with their information in the private sector or the public sector? Does that make any sense?

Dr. Michael Geist: I think it's a good point. It would make for a really interesting, lengthy discussion. Depending on where you go around the world, the perspective on the kinds of privacy protections you should have and the import of either the private sector side or the public sector side varies. There are places where there is more trust of government than there is of the private sector, so there is a tendency to think, "Well, at a minimum I need to hold a very high standard on the private sector side because I'm less trusting of them."

I was in Europe earlier this year with a group of digital civil liberties groups. In that kind of context, a lot of the talk was on surveillance. When they were asked what they were most concerned about, it wasn't the NSA, let's say, but it was companies like Google. They were much more concerned about what the private sector side was doing. If you go to other places, perhaps south of the border, I suspect there is more trust of some of the companies with information than there is of government. I think the answer to that varies. Here in Canada, I'm not sure. We probably fall a bit into the mushy middle. I think we have a fair amount of trust of both, probably more trust of government than we do sometimes of companies.

Regardless, in terms of where the law lands, I'd come back to where I started earlier today, which is that I think there are benchmark standards, principles that by this point in time are fairly tried and true and are seen as what a modern privacy law has. The Privacy Act doesn't have them. PIPEDA certainly does a better job of reflecting them. I don't know that these have to be identical. We've spent an hour and a half now talking about some of the nuances that exist in the public sector side that may not be matched in exactly the same fashion with respect to the private sector; nevertheless, some of the core principles remain largely the same, if we're talking about privacy rules that provide people with at least the appropriate level of confidence about how their information is collected.

In that sense, today, it's pretty clear one of these is not like the other. It's the Privacy Act that is in real need of updating.

The Chair: Mr. Fraser.

Mr. David Fraser: Actually, if I can be very brief, I think one of the significant needs for Privacy Act reform is the change in the expectations of individuals with respect to what privacy is, what it's about. I think that change was informed significantly by the influence of PIPEDA. That is the standard by which people expect their interactions with business to operate. I do think you should line those up as best you can so that consumers' and citizens' privacy expectations are generally the same and are accorded the same amount of respect in each. They don't map perfectly, but there's a reason they're called fair information practices and principles. To the extent that those principles can be expressed in a statute regulating government, that should be the goal.

● (1235)

The Chair: Mr. Erskine-Smith.

Mr. Nathaniel Erskine-Smith: Thanks very much. I want to pick up on what Mr. Calkins was pursuing.

In the private sector, we talk consent; in the public sector, presumably we're going to talk necessity of collection. But when it comes to secondary use, in the private sector we talk consistent use with that initial consent; in the public sector, there are a number of different ways to think about this now.

So you can talk consistent use, you can talk compatibility, requiring some direct connection, and you can talk about necessity and imposing some sort of proportionality requirement. I would be interested in your thoughts as to which of these standards we should be looking at on secondary use.

Mr. David Fraser: It's difficult to come up with a one-size-fits-all, but I do like the necessity approach. It has to be reasonably necessary for a legitimate operating program of the government institution to collect it in the first instance, and obviously that's the purpose that informs the use to which it can be put. You don't necessarily want to bake it in too much, but you do for the private sector. The private sector has to identify the purposes to the individuals, obtain their informed consent, and if they want to use it for any other purpose than the one that they've informed the person about, they have to go back and get consent.

Mr. Nathaniel Erskine-Smith: Do you think it would be too broad then to say, after the initial collection of information, that a department could share that information provided it was for an important government objective for another department, it was necessary for that use, and it was proportionate to that use?

Mr. David Fraser: There may be another way of thinking about it, because when you have one institution disclosing and you have another institution collecting, you might frame it so that for the institution that's obtaining it, it needs to be necessary for their legitimate operating program. There should be enough of a connection between the two.

There may be other mechanisms, for example through an order in council or something else like that, if it's out there, but be mindful of the fact that some things that have been seen to be relatively innocuous have had significant privacy consequences. I don't remember how many years ago it was now, but I recall that HRSDC wanted to bring together a number of databases related to programs that it operated. One could easily say it was all collected by the same department for the same general purpose of providing benefits, but there was in fact an advantage, a privacy advantage, of keeping CPP stuff over here, and EI stuff over there. All of sudden, you create what they call a longitudinal database. It would be from cradle to grave in one database. You could say that those are directly connected, but overall the privacy impact of that is that you've created a Big Brother database.

You want to be very careful, to make sure that the decision-making takes those sorts of things into account and there's visibility and transparency, because these things shouldn't be happening in the shadows.

Dr. Michael Geist: David's answer is an excellent one. I think there's been a bit of a theme about the need for some amount of flexibility here. We've had it on a number of the kinds of issues where, once you start coming up with real-world examples or potential real-world examples, it starts getting more and more difficult to come down with a specific response.

Flexibility sometimes can be a bit of a feature, not necessarily a bug. There is value in that flexibility. What then becomes essential, though, if we recognize that there is going to be that flexibility, is how you ensure that you have appropriate oversight and review as part of that process, and transparency more broadly, so that at least we understand how some of these things are being interpreted, and can better understand whether or not it's consistent with what many people would think is reasonable.

Mr. Nathaniel Erskine-Smith: To put it another way then, because I think PIPEDA, with a principle-based approach, is a good one, if we talk about the necessity principle, and you're both advocating that be included, would a proportionality principle also be an important principle to add with respect to, especially, secondary use, and maybe even initial collection?

Mr. David Fraser: I would, in terms of it. I think it's difficult. I don't envy the legislative drafters' task of trying to articulate that. Courts have consistently talked about proportionality, and it's far more nuanced than what lends itself to black-letter law, but I do think that is in fact what needs to be taken into account.

Is the benefit to government operation or the country as a whole proportional to any trade-off in privacy? I think those are questions that should be asked on a regular basis.

A privacy impact assessment provides a really good framework for asking all those questions, surfacing unintended privacy consequences, and forcing the decision-maker within government to think this might be something we can mitigate this way, or maybe we don't need all that sort of detail. But without that methodology to systematically address it, very easily those nuances can get lost and you're not making the best-informed decisions.

● (1240)

Mr. Nathaniel Erskine-Smith: Thank you very much.

The Chair: Colleagues, that brings to a close our questions.

To our witnesses, as we continue on with this discussion, we see why it's been so long since somebody's been able to come up with some legislation that we'd be comfortable putting in front of Parliament. We thank you. We hope that continued efforts on everyone's part here results in an updated piece of legislation. I know that you probably both stand ready to assist the committee should we ask for further assistance on this matter. Thank you very much.

Colleagues, seeing that there's no other business, this meeting is adjourned.