HOUSE OF COMMONS
CHAMBRE DES COMMUNES
CANADA

Standing Committee on Access to Information, Privacy and Ethics

ETHI • NUMBER 029 • 1st SESSION • 42nd PARLIAMENT

EVIDENCE

Thursday, October 20, 2016

Chair

Mr. Blaine Calkins

Standing Committee on Access to Information, Privacy and Ethics

Thursday, October 20, 2016

● (1100)

[*English*]

The Chair (Mr. Blaine Calkins (Red Deer—Lacombe, CPC)): I call the meeting to order

Welcome, everyone. It's great to see you. This is the 29th meeting of our committee. We're continuing on with our study of the review of the Privacy Act.

We have only two witnesses today. We lost a witness, unfortunately, and we hope everything goes well, but we're still very pleased to have, from the Centre for Law and Democracy, Michael Karanicolas, senior legal officer. We also have Mr. Vincent Gogolek—no stranger to this committee—who is the executive director of the B.C. Freedom of Information and Privacy Association.

Friends, normally we have about a 10-minute opening statement and then we proceed to rounds of questions by all members. We try and encourage every member of Parliament to have an opportunity to ask questions.

Michael, are you ready to go? Is that okay?

Mr. Michael Karanicolas (Senior Legal Officer, Centre for Law and Democracy): Certainly.

The Chair: I usually go in the order in which they appear here, and your name appears first. I think this is your first time appearing before our Parliamentary committee. We welcome you and we look forward to hearing from you and having a discussion.

The floor is yours, sir.

Mr. Michael Karanicolas: Thank you very much for this invitation.

To give you a bit of background on my organization, the Centre for Law and Democracy is an NGO based in Halifax that works to promote foundational rights for democracy. Most of our work is international, but it is a Canadian-based organization. We work here as well.

Our general focus is on freedom of expression, but that has increasingly taken us into privacy advocacy in recent years because there is a growing consensus about the broader importance of privacy to freedom of expression. This was noted by the UN Special Rapporteur on freedom of expression in 2013 and in the 2014 report by the Office of the UN High Commissioner for Human Rights.

The right to privacy, of course, is also internationally recognized as a human right on its own, protected by article 12 of the Universal Declaration of Human Rights as well as the International Covenant on Civil and Political Rights, which Canada has ratified.

I'll add that the value of a right like privacy must be considered in broader and systemic terms, rather than just by virtue of one's own sense of the private. Too often, as part of our advocacy, we've come across a statement to the effect that, “Well, I personally don't care too much about privacy or the integrity of my information. I'm not particularly a private person. I don't have much to hide, so I don't see these as important issues to address.” To me, that thinking is analogous to a person saying that because they're not personally religious, they feel no need to safeguard freedom of religion. There are broad social benefits that accrue to everyone by having a robust and properly protected right to privacy.

With regard to the current recommendations that are being discussed, we generally support what's been put forward by the OPC. For the sake of brevity, I'm not going into detail on all of the recommendations, but any of the ones that I don't specifically mention, we do support.

To start off, we strongly support the need for greater clarity around information agreements made under paragraphs 8(2)(a) and 8(2)(f) of the Privacy Act. There's a global trend among governments, and that includes our neighbours to the south, to adopt an approach to privacy that extends some protections to their own citizens and virtually none to foreigners. In this context, Canadians have to rely on their government to safeguard their privacy rights in dealings with external actors.

Clarity, transparency, and robust oversight are key ingredients to this, and the OPC's recommendations are a necessary step along that path. We would actually go beyond the OPC's recommendations and suggest that these agreements should be public and should set clear limits as to the purposes for which the disclosures may be made. There should also be a system of disclosure when these conditions are violated and effective remedies for those individuals who are affected.

CLD supports the recommendation that there should be an explicit necessity requirement for the collection of personal information. I would note that this is not just about protecting against the privacy infringements that result from the collection and processing of the information itself. Over-collection magnifies the threat to data security, since the ease of storing massive amounts of information can turn public agencies into a bigger target for hackers. Security experts have long argued that data minimization is among the most important defensive measures in protecting personal information.

When the United States Office of Personnel Management was catastrophically hacked last year, releasing, among other things, the results of background checks for millions of current and former employees, one of the big questions that security experts asked was why on earth they were warehousing all this information. There's no such thing as perfect security, but by working to manage and restrict the amount of information held, an agency can proactively mitigate the damage of a breach if and when it occurs.

Expanding the commissioner's ability to share information with counterparts domestically and internationally is also a good idea, particularly in light of the dynamic nature of global information flows. The Internet poses a significant challenge to traditional understandings of borders and jurisdiction, which makes it difficult to safeguard rights online. When a guy in Saudi Arabia, a country where adultery is a criminal office, has his Ashley Madison profile leaked due to negligent safeguards by that company, where does his remedy lie? That's to say nothing of the almost 1,300 Ashley Madison users who identified themselves to the service as gay and whose log-in information originated from countries where homosexuality is criminalized.

● (1105)

There are very serious international consequences to these kinds of leaks. The Internet is a borderless place, and any agency that seeks to protect the rights of Canadians online needs to coordinate internationally.

CLD supports the idea of stronger transparency on reporting requirements for government institutions. However, rather than setting specific standards in the act, we would suggest leaving the specific scope of that to either the Privacy Commissioner or the Information Commissioner, to be defined through their regulations. That is in order to allow them to deal with emerging issues as they arise without having to reform the law.

There are two areas where we take issue with the recommendations. One is regarding the exception in the Access to Information Act for personal information, which the Office of the Information Commissioner has argued should be narrowed, so that it only applies to information whose disclosure would create an unjustified invasion of privacy. This would transform the current class exception for personal information into a harm-based exception in line with international better practices.

The OPC has voiced opposition to narrowing the definition in the matter in the way that the OIC suggests. CLD strongly supports the OIC's position in narrowing the definition.

The first reason is that there are enormous amounts of personal information whose disclosure is not sensitive—for example, where the information is already broadly publicly available—and as a consequence there would be no material harm in its disclosure. A harm test, which is what we're advocating, clarifies that information should always be disclosed in these kinds of cases. This prevents undue delays in processing requests and is a core earmark of good access to information legislation.

Second, in its submission the OPC has advocated for a formula that inherently tilts the scales in favour of privacy by requiring that a public interest override to have the information disclosed would only kick in if the interest in disclosure would clearly outweigh the privacy interest. This is an incorrect approach. The right to information is a human right, is broadly recognized internationally, and is also recognized as a limited and derivative constitutional right. It should be balanced against the right to privacy on equal terms.

Regarding order-making power, CLD doesn't necessarily oppose this idea. At the same time, I'm not particularly convinced by the argument for order-making power based on a necessity for parity between the Information Commissioner and the Privacy Commissioner. There are important differences between these two institutions, the main one being that the OIC's reviews are almost entirely aimed at public bodies, whereas the OPC has an oversight role over both public and private bodies.

This is a substantial consideration when you're talking about providing the agency with a bigger stick to wield. It heightens questions about procedural fairness and investigations, which the OPC has itself identified as a challenge.

There is also the question of collaboration and relationships with private sector respondents and whether this would impact the ability of the OPC to seek informal resolution or whether enhanced powers would make it more likely that private sector interests, if contacted by the OPC for an investigation, would put up a defence and lawyer up.

Again, that's not to say that we're opposed to order-making power. To me, it comes down, first of all, to whether order-making power is necessary to compel compliance with the recommendations that are being issued and, second of all, to whether it would make the OPC more effective in its oversight role. Would it create a greater impetus for organizations to follow their recommendations? Would it turn it into a stronger body, or would it further delay the process by making companies more defensive through the investigations? I don't know the answer to that question, but I think it's important to think about the issue in those terms.

It's also worth considering in the context of the statement by the OPC that most institutions do eventually agree to their recommendations, though there can be lengthy delays. Against that backdrop, obviously the delays are a legitimate concern, but if that's the major issue, I'm not entirely certain how order-making power would solve it more effectively than the hybrid model that had been previously suggested.

Without making a statement against order-making powers, I want to frame the discussion that way and have the discussion over questions of efficacy and necessity, as opposed to parity between the different institutions.

That's what I have in terms of our opening statements. Thanks very much. I look forward to engaging.

● (1110)

The Chair: Thank you, Mr. Karanicolas.

Now we go to Mr. Gogolek for up to 10 minutes, please.

Mr. Vincent Gogolek (Executive Director, B.C. Freedom of Information and Privacy Association): Thank you, Mr. Chair.

Thank you to the committee for inviting us back once again to speak on an issue of considerable public interest and public importance.

It's a relief to see that this committee is examining the Privacy Act in the same general time frame as the Access to Information Act, because the two, of course, were introduced together. It's important for them to be looked at by the committee at the same time. I much appreciate that you're doing it in the way you're doing it. I think is a very good approach.

You have our written submissions, which deal with each of the Privacy Commissioner's recommendations. We also have a few thoughts of our own at the end. I'll follow the example of—

The Chair: Excuse me, Mr. Gogolek.

Just for clarification of committee members, the submission by Mr. Gogolek is in translation right now, and we'll be getting it shortly.

Thank you, Mr. Gogolek.

Mr. Vincent Gogolek: Okay, thank you for that.

In any event, I'll just deal with the points that I think need amplification. There are many of the commissioner's recommendations that we're in agreement with, and you'll see that in the submission when it finally emerges.

Generally I think that in the testimony you've heard so far, it's common ground among the witnesses that the Privacy Act is outdated, antiquated, and in need of complete overhaul to ensure that Canadians' privacy rights are properly protected. This should also be done to bring the act into closer harmony with not just the more modern and more protective privacy laws, but also with its federal private sector equivalent, PIPEDA, which is administered by the very same commissioner.

Of course there are differences between the public and private sector, obviously. However, for Canadians who are going to the Privacy Commissioner to seek remedies or to figure out what their rights are or what the Privacy Commissioner can do for them, I'm sure it's very confusing as to why the remedies in terms of the public sector are so very different, and the procedures so very different, from what they would have in terms of PIPEDA. We urge you to make the changes required to end this disparity and confusion.

I'll now proceed to quickly go through the recommendations of the commissioner.

First is the requirement to put in an explicit necessity requirement for data collection. This is the standard set out in B.C.'s Freedom of Information and Protection of Privacy Act, as well as a number of other laws. The concept has received considerable interpretation, judicially and quasi-judicially, so its operation is well understood. We recommend that this be explicitly included in the act. We agree with the commissioner.

We'd also like to point out that one of the many criticisms of last year's Security of Canada Information Sharing Act, which was part of Bill C-51, is that it allows information on the lowest possible standard—that is, that the information is relevant to a receiving organization's jurisdiction or responsibilities in relation to activities that undermine the security of Canada in relation to detection, identification, analysis, prevention, investigation, or disruption of those activities.

We're of the view that this law is actually subordinate to the Privacy Act. However, the government's own background paper to the green paper, which is now currently also the subject of consultations, is actually contradictory on this point. In one place it says yes, it does override, and in another place it says no, it doesn't, that it's subject to other legislation, including the Privacy Act. It seems that the government itself is not entirely clear on this point. Given the weaknesses in terms of the lack of an explicit necessity clause in the Privacy Act, we think this would go some way toward helping resolve this ambiguity.

I'd also like to point out that the CSIS act uses the standard of necessity as well.

In terms of expanding judicial recourse and remedies under section 41, we support this recommendation. We would note that the B.C. legislative committee that recently reviewed our province's act has recommended that penalties be increased in order to focus the minds of those who may either not be paying proper attention to privacy rights or would ride roughshod over them.

One example of why this is necessary is the case of Sean Bruyea, a veterans advocate who had his personal information, which was held by Veterans Affairs, accessed hundreds of times by hundreds of individuals, including his financial, medical, and psychiatric records. Some of those records actually ended up in not one but two different ministerial briefing notes.

● (1115)

Mr. Bruyea was eventually compensated, but that was because he had already brought an action for damages for violation of his charter rights. That's an exceptional action, and we agree with the commissioner that there should be a broader scope and a broader availability of sanctions, including damages, under the Privacy Act.

In terms of the ombudsman versus order-making power versus hybrid, we see that the Privacy Commissioner himself, last month, has come around to the view that order-making power would be preferable. This is the view we have long held and the view we have also put forward in terms of the Information Commissioner. Both of these officers of Parliament should have order-making powers.

With regard to the discretion to discontinue or decline complaints in specified circumstances, this is understandable and necessary for the economy of public resources in cases where there is a request or a demand for review that is frivolous, vexatious, or done in bad faith. However, it should be restricted to those narrow points.

In terms of exceptions, the commissioner's recommendation 16, we agree with the Information Commissioner on this point. We have for a long time been in favour of exceptions to release under the ATIA being harms-based, and that would include personal information. We are also not in favour of this being discretionary.

I have three additional points that I would like to raise. First, I'd like to point out that in British Columbia our public sector act has a domestic data storage requirement, something that does not exist at the federal level. Again, this requirement was recently supported by the committee reviewing our act earlier this year, and also by the Government of British Columbia. We would commend this to you as something you may want to look at, in terms of B.C.'s experience.

Second, in 2008 the commissioner made a recommendation to eliminate the stipulation that the act apply only to recorded information. We think that was a good idea in 2008, and we still think it's a good idea. Although the commissioner hasn't mentioned it this time, we think it's an important change.

Third, something that we're seeing increasingly in the public and private sector in terms of decision-making is the use of data mining, and especially the use of algorithms to either supplement or entirely replace decision-making by human beings. Data is run through a program, and a recommendation, which humans may be reluctant to overrule, comes out. These rulings oftentimes have very serious effects on individuals, especially in terms of social services or benefits or things like that.

Something we have found over the years is that there is a great deal of resistance by private sector and public sector bodies that are using these algorithms and technologies to provide any kind of access to their workings, or even the basis on which these things work.

● (1120)

This really contradicts what happens when you have a human decision-maker. They normally have to provide reasons. There's something you can look at to figure out how they got to their decision. If this approach is replaced by a black box that has unknown data coming in from an unknown variety of sources and a recommendation coming out at the end, the person whose livelihood, finances, business, and other interests may be affected should have a right to see that. I think that has to be in the act.

I now look forward to your questions.

The Chair: Thank you very much, Mr. Gogolek.

We're now going to go to our first round of questions, which will be seven minutes for questions and answers for each member, and we're going to start with Mr. Saini.

Mr. Raj Saini (Kitchener Centre, Lib.): Good morning. Thank you both for coming here.

Mr. Karanicolas, I was reading a piece that you wrote. I think you called it “Travel Guide”, and you talked about data retention obligations.

I want a differentiation from you, if you could highlight that for us, between the private sector and the public sector. You wrote in that piece about certain governments around the world, whether Thailand or India, having certain data retention obligations, and you wrote about an issue in Europe, where they tried to require service providers to retain data, but certain states hesitated.

When we look at the private sector, we see that consent is required when they collect data. Their collection of data tends to be more targeted, as opposed to government's, where the data tends to be broader or more diffuse. The government has an obligation to collect data. There's the CRA, and things like that. How do we ensure that the government is able to retain that data and yet also ensure that over-collection does not occur?

Could you highlight some of the things that we could improve, as compared to the private sector, and how we could go about that?

Mr. Michael Karanicolas: Thanks very much.

First of all, it's great that you found that work, “Travel Guide to the Digital World”.

I completely agree that there's a big difference between information collection that happens in the private sector and information collection that happens in the public sector. Information collection by the public sector has a lot more potential for abuse and needs to be monitored much more carefully, partly because governments can get up to.... I work a lot in repressive countries, so I know governments can do much nastier things with private information, personal information, than private companies can. Governments have extraordinary levels of power, and the ability to misuse that information is much higher in the public sector than in the private sector. We take a much more wary approach when we talk about government collection of information.

You also noted the consent model. When you talk about consent, that's another issue. You can choose to delete your Facebook account and you can choose to delete your Gmail account, but you can't really choose to stop paying your taxes. You're a Canadian. You're in the system. It does also change the dynamic quite a bit.

I will also say that the consent model for collecting information in the private sector does need to be thought through very carefully, and I would argue that the current consent model is broken. Nobody reads their terms of service and nobody understands their terms of service. There's a bit of a vicious circle. The fact that nobody reads their terms of service means that the lawyers who draft these terms of service are incentivized to draft them in incredibly broad and vague ways in order to make sure they cover every imaginable use. There's no incentive for them to clarify the terms or to limit the actual uses in their terms of service, because they know that the users don't care. Then the fact that these terms of service are drafted in such a broad way makes it very difficult for people who want to read and understand them to actually get an understanding of what they mean. That, in turn, disincentivizes users from actually reading and engaging with them.

While I do agree that information collection in the public sector needs to be watched more carefully, I don't think that this consent-based model is necessarily the answer to the private sector doing whatever they want. Actually, I think that stronger and clearer rules around how private sectors use people's information are very badly needed. I think that the current model is not providing adequate safeguards.

I've seen estimates that if you were to read every terms of service document that you were presented with, it would take something like 200 hours out of your week. It's not practical for people to actually be their own safeguards on this issue.

Sorry. I realize I am straying a little from the question.

● (1125)

Mr. Raj Saini: Go ahead, but there's another question I want to ask on that aspect.

Mr. Michael Karanicolas: Just quickly, in terms of what public bodies should be doing, I'm not a data security expert. You have security people who will tell you the areas you need to improve. The main thing that I would say is data minimization.

You can do what you can to try to make yourself as secure as possible, but the most important thing is that you can also make sure you manage your information, such that if and when there is a breach, you don't open up all this information that you should have deleted years ago.

Mr. Raj Saini: The other question I have for you—and you mentioned this also about privacy agreements—is that right now we're part of the Five Eyes intelligence group. Within that regime, there is some level of confidence that with the countries that are part of that regime—because they're developed governments—information shared across borders would be retained in a way that would be somewhat safe or private.

However, we also have transactional agreements with other governments when it comes to CRA and things like that. In Canada we have a robust regime of preventing data sharing, maybe even among government agencies, but that information can leave our border and go to a different country that has a different set of rules. They may have the best intentions, but their rules are not as robust or as developed as ours. How do we protect against that?

Mr. Michael Karanicolas: First of all, while sharing information among the Five Eyes is not the same as handing that information over to Egypt or Saudi Arabia, I think that abuses do take place and have taken place within our Five Eyes partners. There's clear evidence of that.

I'll particularly point to the U.K. and the fact that GCHQ has operated far beyond the kinds of limits that we've seen in other agencies. The U.K. is now talking about pulling away from the European Court of Human Rights. I think there are very serous concerns among our Five Eyes partners, so I wouldn't necessarily start from that perspective.

In terms of actually controlling the information, I think the best thing that can be done is to spell out very clearly and publicly the kinds of information we are willing to share, to have an open public debate about it, see what Canadians are and are not comfortable with, and have agreements that specifically reference those uses of information, with consequences if those agreements are not adhered to. You can spell out specifically in the agreement if it goes beyond this agreed-upon measure.

Mr. Raj Saini: You also mentioned remedy.

The Chair: We're well past seven minutes now.

Hold that thought, Mr. Saini. I'm sure we'll have time to finish up on this later on.

We'll now to move to Mr. Jeneroux, please.

● (1130)

Mr. Matt Jeneroux (Edmonton Riverbend, CPC): Wonderful. Thank you both for being here.

Mr. Gogolek, we've changed our committee time a little, so hopefully it was a bit easier on you coming from British Columbia.

Mr. Vincent Gogolek: It was a bit early.

Mr. Matt Jeneroux: It was, wasn't it, for all of us?

Mr. Karanicolas, I want to ask you a question, hoping that it clarifies some things on our end.

Your organization appeared before us at the meeting on the Access to Information Act, which we just studied, and your colleague provided strong testimony with regard to increasing the right to information. In fact, your organization reminded the committee that the right to information is a human right under international law. Now our committee is discussing the other side of the question, the laws that protect privacy.

I'm wondering how your organization views the balance that must be struck between providing as much access to government information as possible while also protecting the privacy rights of Canadians.

Mr. Michael Karanicolas: I absolutely agree that there does need to be a balancing between those two, but this is not the only instance in which we balance rights against one another. We balance privacy against freedom of expression when talking about regulation of the media and what they should and should not be able to publish. We balance national security against privacy when we talk about appropriate scopes for data collection and data storage.

Balancing rights against each another is something that democracies have to do. In this case, with specific reference to the Access to Information Act, what we want to see is a balancing, on equal terms, of the right to privacy against the right to access to information to see where the greater public interest lies.

The general way that this is structured in better practice jurisdictions around the world is to have an exception with the Access to Information Act to say that information will not be disclosed if its disclosure would cause harm to personal privacy. Beyond that, this exception, and all other exceptions, will be subject to a public interest test whereby, if the public interest and disclosure override the privacy interest, then the information should be disclosed regardless of the exception.

Mr. Matt Jeneroux: Given that technology continues to evolve and that the last time the act was updated was in 1983, and it's now 2016, what are your thoughts—both of you hopefully can weigh in on this—on how we keep up with current technology now, while knowing that in 2017 or 2018 there's probably going to be something else that we will also need to keep up with? I guess it's the "we don't know what we don't know" argument.

How do you suggest we consider that when it comes to the act?

Mr. Vincent Gogolek: It's a very important question because, as you point out, technology moves very quickly. Things that were around in 1983, such as telecopiers, don't exist anymore. That's an entire category of one of the standard things that was used back then.

This shows the importance for legislators of writing laws at a relatively high level, keeping them principle-based and technology-neutral. That's so you're dealing with the concepts of things like "personal information transmission", as opposed to "faxing" or "using teletype", or "specifying". Unless there's some very good reason—a particular technology has a very particular problem or issue or feature that needs to be dealt with—keeping the laws that you come up with at that higher level and without specifying a specific technology, unless it is a necessary requirement to deal with that actual problem, I think is the way to go.

Mr. Michael Karanicolas: I would add that regular reviews are a good idea. I think five-year reviews have been among the recommendations for both the Information Commissioner and the Privacy Commissioner. I think they are a great idea.

You mentioned that it's been over 30 years, and there haven't been any amendments. Canada was, I think, the eleventh country in the world to pass an access to information law. There are now, I believe, 113 laws that have been passed around the world, so standards have advanced tremendously in the intervening years. There's an important need to keep up, so regular reviews written into the legislation are a very good idea.

I would add that I completely agree with writing things in a technologically neutral fashion. That's always a good model for legislation generally.

I would also mention that progressive implementation of proactive disclosure obligations can be a good measure, as we see in a lot of different laws in which obligations for what should be disclosed ramp up over time. We do see this happening to an extent with the government, which is pioneering new open data initiatives and expanding new ways to engage with people. That is great.

However, what some countries do is that they allow the Information Commissioner—and I sort of hinted at this in my presentation—to set regulations about what levels of disclosure should be expected, and then those obligation levels can level up over time.

● (1135)

Mr. Matt Jeneroux: Mr. Gogolek, quickly, do you have a time frame in which you prefer to see the statutory review, or a review of any sort, take place?

Mr. Vincent Gogolek: We would agree with the commissioner in terms of five years.

In B.C., we have a six-year term. I believe that this committee recommended a five-year review for the Access to Information Act, and I think one should be reviewed the way you have been doing it this year. They should be looked at on the same time frame.

The Chair: We now move to Mr. Blaikie for up to seven minutes.

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

I want to return to the question of order-making power.

Mr. Karanicolas, I think you made a distinction between—and I don't want to be putting words in your mouth—the appropriateness of order-making power for the public sector and the appropriateness of order-making power for the private sector.

I wonder if you could speak a little more to that and answer the question of whether it would be possible, and furthermore advisable to.... I mean, if there are issues with order-making power with respect to the Privacy Commissioner's obligations under PIPEDA, could you have order-making power under the Privacy Act for the public sector and a different model for the private sector? Does that make sense? Can you kind of flesh out some of the details?

Mr. Michael Karanicolas: I'll reiterate that we're not opposed to order-making power. We're on the fence about it, and to me it seems like an issue of efficacy more than anything else. I'm inclined to defer it to the Privacy Commissioner, if they think it will help them to do the job better.

I don't think the argument that if one commissioner has it, therefore the other commissioner has it holds a lot of water with me. It's more that you look at the commissioner's specific mandate, you look at their success in implementing their recommendations, and you look at the tool kit they have available to them and the needs they have. You design particular powers around that. These commissioners are structurally similar in a lot of ways, but have very different mandates, so I do think they require different considerations. That was the way I was trying to frame it.

With the divide between public sector and private sector, there are enhanced procedural considerations if you want to talk about an organization that is levying fines, and potentially large fines. There have been a lot of pushback complaints from the private sector about the anti-spam mechanism, about CASL, and the way fines have been levied there. I think people in the private sector are a bit concerned about that.

I have heard from private sector people on the argument I made about private sector interests being less likely to co-operate with an agency that has order-making powers. You hear that from people in the private sector. You have to take it with a grain of salt because, of course, they don't want to be overseen by an organization that has power to fine them. They would prefer an organization that doesn't have those powers to be overseeing them. There's an obvious interest there, but I also don't think it can be entirely discounted. I would defer to the Privacy Commissioner if the question is framed specifically on efficacy.

When you're limiting the order-making powers so that they only apply to government, I think if you did it in that way, then it would certainly limit some of the concerns, and that would make the argument for parity a little bit better. If you look at the Privacy Commissioner's role specifically with regard to interacting with public bodies, you see it is quite similar to the Information Commissioner's role.

However, the Privacy Commissioner also needs to have the tools available to properly protect Canadians' privacy, particularly in the private sector, particularly when you look at the failures of the consent-based model, which I went into a little bit before. I do think there need to be stronger rules in place. Whether that's done through orders from the Privacy Commissioner, whether it's done through legislation or regulations, or whether it's done through recommendations, I'm not sure, but I do think there needs to be greater clarity.

● (1140)

Mr. Vincent Gogolek: I have a brief point about the private sector, but it relates to all of it.

In the private sector, of course, we have two different sets of regimes. We have PIPEDA, which is the federal regime, and then we have substantially similar regimes in a number of other provinces, including British Columbia, which we're familiar with. You have the unusual situation of the commissioner making recommendations under PIPEDA, while in British Columbia, our commissioner issues orders.

We were involved in a case in which an insurance company had been ordered to get explicit consent from their customers for use of their credit information to determine the level of their premiums, so we had an actual order. Eventually another complaint was brought under PIPEDA from Ontario, a PIPEDA-level resolution was reached, and the organization ended up doing this at a national level.

It could create an interesting situation. You could have one substantially similar jurisdiction where there's an order in place and an organization or a company is required to do something, but not in the PIPEDA jurisdiction.

This is another reason we are in favour of order-making power for the Privacy Commissioner, both public and private.

Mr. Daniel Blaikie: Do I have a bit more time?

The Chair: You have one minute left.

Mr. Daniel Blaikie: In terms of providing a public education and research mandate for the office, I didn't hear disagreement with that recommendation in either of your presentations.

I'm wondering if you have a sense of what exactly you take that to mean and what you think would be a reasonable implementation of that mandate, so that we can try to get a sense of the resources involved for something like that.

Mr. Michael Karanicolas: This also parallels a recommendation that we made for the Information Commissioner.

To me, it's about a gap in understanding among Canadians about what privacy is and about the changes that have occurred as a result of digitization, which have dramatically changed people's relationship with personal information. It's about giving the Privacy Commissioner a stronger role in promoting privacy. They do that in the private sector. I think that because there are greater concerns among the public sector, it's important to extend it to that sector.

In terms of specifically how that would work, I imagine it would be parallel to the way it currently works in private sector promotions. They could be sponsoring research, sponsoring conferences, in order to promote engagement by public agencies—or via academics or NGOs—with the public in terms of getting them to understand their privacy rights.

It's generally a parallel, I think, to the way it works currently.

The Chair: I have to cut it off right here, right now, but keep the thought. We'll have an opportunity.

Mr. Massé, I believe the floor is yours.

[*Translation*]

You have seven minutes.

Mr. Rémi Massé (Avignon—La Mitis—Matane—Matapédia, Lib.): Thank you, Mr. Chair.

I'd like to pick up on your discussion with Mr. Jeneroux and talk about the evolution of technology and the measures needed to make sure the legislation keeps up with new technologies. Obviously, it's a very likely scenario.

Mr. Gogolek, you piqued my curiosity earlier when you were talking about data mining. It's increasingly being used to make much more specialized decisions a lot more quickly. You said there was a genuine concern when it came to data mining. It's possible to take a black box, fill it with a bunch of data, and have it make more specific decisions.

How would you recommend we take that reality account, to make sure the legislation sets out a better framework and to give individuals access to what's inside that black box? I'd like you to elaborate on that.

● (1145)

Mr. Vincent Gogolek: That's a very technical question. As far as the technology inside the black box goes, governments or companies sometimes argue that the information is proprietary and therefore confidential, that it would reveal business practices. According to them, competitors could benefit from disclosure of the information.

It essentially comes down to replacing or supporting decisions made by humans with recommendations that are practically decisions in and of themselves. In a number of cases, in fact, it would be very tough for an individual to challenge what the computer has deemed a good decision. In order to challenge what comes out of the black box, a person has to be very confident in themselves and their expertise. That's key.

When people make decisions, they normally have reasons for making them. The data they used to arrive at their decision are known. It's important to keep that option open It's not a good idea to create a situation where it isn't possible to reconsider what the decision-maker did. If the decision came out of the black box, it's important to know that.

That doesn't necessarily mean knowing exactly how the circuits are connected, technology-wise. Rather, it means knowing which data were part of the data mix. It's actually a matter of knowing, overall, how the data were organized to arrive at decision *x* or *y*.

Mr. Rémi Massé: Absolutely.

There's something I find a bit troubling with this. But it's not a concern I have vis-à-vis the federal government, since it's always a bit behind the private sector when it comes to technology or technology development, in my view.

Mr. Karanicolas said that the consent model was so broad and vague that just about any information could be collected without the user even knowing it. The private sector bases its collection of data on consent that is provided initially.

Given that vast quantities of information can be collected, with consent, and fed into a black box, how can we protect Canadians in the future, through the amendments to the act?

Mr. Vincent Gogolek: The commissioner made two recommendations, one being the introduction of a necessity test, which isn't in the current legislation. It is, however, in our public sector act here, in British Columbia. It's very important because it raises the requirement level. The data collection has to be necessary. Information can't be collected simply because it would be beneficial to have. That isn't permitted; the information has to serve a purpose. That is why, then, the recommendation is important.

Mr. Rémi Massé: Thank you. That's much appreciated.

Mr. Chair, I'm going to give the rest of my time to Mr. Long, who also has some questions.

[*English*]

The Chair: You have a minute and a half, Mr. Long.

● (1150)

Mr. Wayne Long (Saint John—Rothesay, Lib.): Mr. Karanicolas, I want to talk to you about some of your tweets on Twitter. I want to talk about Hadas Gold.

Hadas Gold is the journalist who has come under some public scrutiny, I guess, and I think some very bad things are happening to her. You made some comments saying that you don't believe it's Twitter's responsibility to police that. Can you elaborate on that situation? Obviously there has been a threat made against her. What do you think the solution is to that? What regulations would you put in to control something like that?

Mr. Michael Karanicolas: That's going to be very tough to do in one minute.

Mr. Wayne Long: It is. I know. I'm sorry.

Mr. Michael Karanicolas: What I will say is that situations like this need to be taken more seriously by the police, and the reason I phrased it the way I did is that I think that when threats are made against journalists, it is a threat to democracy, and I think that these need to be taken more seriously.

In terms of Twitter's specific role in it, I think companies need to be given the freedom to manage the platforms the way they want to. If a company wants to say that they're a family-friendly platform and they're going to moderate very heavily, I think that's a fair point. If a company wants to say that people can say whatever they want and the only time they're going to take material down is if it's specifically illegal and they are ordered to do so by the state, I think that's also a fair position for them to take.

As long as there's a multiplicity of different platforms available and people can choose how and where they want to engage, I think that's a fair point in terms of the specific regulations.

Mr. Wayne Long: You would agree that right now that it's a free-for-all.

Mr. Michael Karanicolas: It depends on the platform. Twitter has traditionally taken a much lighter hand, and now they're engaging more heavily because of the pressure they've come under. Facebook has always engaged more heavily, but again, they're coming under pressure. They recently have faced some criticism for deactivating certain Palestinian sites under pressure from the Israeli government. Facebook has faced criticism for deactivating Kurdish websites under pressure from the Turkish government.

It's a very challenging political situation once you expect these intermediaries to be the arbiters of acceptable content. It can also be problematic because in some cases you don't really have a proper appeal mechanism. If the government orders you to make a particular decision—if it says, “This content is illegal, so don't publish it”—you can appeal it. There are all these procedures in place. However, if Facebook is the one that's telling you what is or is not acceptable, there aren't the same kinds of procedural protections there.

This is why I'm leery of governments off-loading that responsibility. Specifically, you see cases—I'll point to South Korea as one—of the government doing this as basically a way to impose censorship indirectly, cases of the government leaning very heavily on tech companies to do the content moderation for them. There are very abusive content controls as a result.

The Chair: Sorry, Mr. Long, but—

Mr. Wayne Long: Maybe we'll continue that discussion next time.

The Chair: Yes. I don't mind going a bit over the time when we're talking about stuff relating to the Privacy Act, but when we're going over time talking about things related to PIPEDA, it makes me excited about the upcoming study on PIPEDA, notwithstanding the fact that the dialogue is actually very informative. Let's try to keep it on the Privacy Act if we can, please.

Mr. Kelly, you have up to five minutes. We'll start the five-minute round right now.

Mr. Pat Kelly (Calgary Rocky Ridge, CPC): Thanks, Mr. Chair.

I as well was intrigued by Mr. Gogolek's discussion of the automated algorithmic decision-making.

My first thoughts when you raised this issue were not around the public sector but the private sector, where the type of decision-making I'm most familiar with from my own career before being elected was in terms of credit. Credit-rating agencies have used algorithmic decision-making...well, not decision-making, but they assign scores to establish probabilities for certain behaviours that are then used to make decisions.

Just so I know what we're talking about, can you give me an example in the public sector, in government departments, and tell me how similar the type of information is that you're concerned about. What departments use these tools, and what decisions are made this way?

Mr. Vincent Gogolek: As for where this would come in, a primary example would be—this is perhaps more provincial than federal—in terms of various types of social benefits or things like training programs.

Mr. Pat Kelly: Let's try the federal one, so that my chair doesn't nudge us back on track.

● (1155)

Mr. Vincent Gogolek: Employment training is one of these jurisdictional areas where there are federal and provincial programs. Obviously, government wants these programs to work well. They want the public funds that are allocated to them to be used efficiently and to get the right people the right training so they can be productive employees and productive citizens. An algorithm is developed such that it can take all kinds of different information about a person and say how likely they are to actually succeed if provided this training.

Mr. Pat Kelly: What you've described sounds more like.... You've mentioned the issue about a human making a decision versus a black box doing it, or about having the courage to second-guess the answer the computer provides, but is that a privacy concern or is that a decision-making methodology concern?

I look back at the situation I'm more familiar with. The fact that a computer assigns a credit score is not where the privacy concern exists. It exists in this: did the person consent to disclosing the information? If they consented to disclosing the information, then decision-makers are free to either sort it out themselves or to plug it into a computer. That's not where the privacy issue comes about. It comes about through either a data leak, which is a separate issue....

Explain the privacy component to your concern around electronic decision-making.

Mr. Vincent Gogolek: The privacy aspect relates to the collection of personal information, the data mining, whereby information is taken from various sources, some of which may be publicly available and some of which individuals or perhaps all Canadians are required to provide to government. Generally, it's provided for a purpose. We provide our income and things to ensure compliance with the tax regime or for other reasons. We provide our information to government, and this is where the requirement for a necessity test comes in.

This is probably also where the commissioner's recommendation about information sharing agreements comes in, because there would have to be some of this if information is being drawn from across government in order to determine eligibility for programs, and it would be important for us to know where this is coming from. We don't have a consent element, really, in the public sector, because there's only one provider and we're normally providing information under compulsion. That's required.

Mr. Michael Karanicolas: Can I just add something?

The Chair: Sure.

Mr. Michael Karanicolas: In terms of collating different types of information, I just want to point out that there can be data sets that used by themselves are relatively innocuous, but when you combine them with another data set, the impact on privacy can be escalated dramatically, so the use does make a big difference in how people's privacy is impacted.

The Chair: Good.

We'll now move to Mr. Lightbound for around five minutes, please.

[*Translation*]

Mr. Joël Lightbound (Louis-Hébert, Lib.): Good morning.

Thank you, gentlemen, for joining us today. Thank you, as well, for the work you do every day.

My first question is for you, Mr. Gogolek. Earlier, you talked about B.C.'s domestic data storage requirement. What is it trying to prevent?

I believe Quebec has similar provisions, requiring that data remain in the province. The objective is to keep the data from ending up under the jurisdiction of another act. Is that correct?

Mr. Vincent Gogolek: That's precisely it. It's a bit of a long story, but we had an extensive debate on the subject in British Columbia around the turn of the century. The provincial government contracted private organizations to provide certain government services, including the medical services plan and the pharmacare plan.

The information in the databank is obviously very personal and sensitive in nature. The company the provincial government hired was American, Maximus. It was also around the time when the USA PATRIOT Act came into force. It sparked a big controversy. Our privacy commissioner at the time, Mr. Loukidelis, was very concerned about what could happen to this kind of personal information and about the possibility of it being subject to American laws, specifically, the USA PATRIOT Act.

● (1200)

Mr. Joël Lightbound: That brings me to another question, while I have two experts in front of me.

Earlier, we were talking about the Five Eyes group. Under Canadian law, spying on Canadians is prohibited without a judicially authorized warrant. However, just about anything goes when it involves foreigners. We are part of an alliance where countries share intelligence. Isn't that a way of getting around what is prohibited under the act?

I'd like you to explain how it works, to the best of your knowledge. I know that all the agreements may not be public. Am I interpreting that correctly?

Mr. Vincent Gogolek: I will answer first, and then, I will leave some time for Mr. Karanicolas to answer.

It's a bit complicated. It is clear that Canadian laws apply in Canada and, in some cases, elsewhere. One of the problems, however, is that the origins of these agencies, the Five Eyes alliance, can be traced back to the Cold War. They were mandated to spy on the communications of foreign militaries in the Soviet bloc, China, and other countries. That was their objective and their job. Obviously, privacy and the protection of personal information wasn't a consideration.

Over the years, the activities of these agencies changed. They undertook other types of surveillance, not just spying on foreign militaries. They now monitor organizations and individuals considered threats to Canada. Their activities are beginning to have a much bigger impact on Canadians and their interests, given the digital world we live in.

Mr. Joël Lightbound: Mr. Karanicolas, where do you stand?

[*English*]

Mr. Michael Karanicolas: Yes, absolutely, it is a loophole that can be exploited, and it has been exploited.

To give you a parallel example, which I think spells the issue out more clearly, you have the United States signing information surveillance agreements with Denmark. They signed an agreement with the Danish intelligence agency and they said, "You can use our networks to spy on anybody outside of Denmark, but you can't spy on Danish citizens with them." Then they made an agreement with the German government and they said, "You can use our networks to spy on anybody outside of Germany, but you can't spy on Germans." It's the same network, so if they're on both points in it, then they effectively get access to everybody's information. It's a neat trick to say, "We're not using your network to spy on you", but obviously it's a loophole that allows the system to be subverted.

As for how the system has functioned, my understanding is that previously Canadians traditionally have not had as strong an oversight over our intelligence services, but our intelligence services tended to respect boundaries much better. The information that I have heard suggests that under the previous Canadian government, that dynamic changed dramatically, and Canada's intelligence agencies became far more aggressive. Not being in a position to personally be able to oversee it, it's difficult to say, but that's the impression that I have.

[*Translation*]

Mr. Joël Lightbound: Thank you.

● (1205)

[*English*]

The Chair: Thank you very much, Mr. Lightbound.

We're almost at six minutes, so we'll now move over to Mr. Kelly, who I believe is going to split his time, possibly, with Mr. Jeneroux.

Mr. Pat Kelly: Perhaps.

I want to ask a question that's a little different from what we've had so far.

We talked quite a bit about the dangers around security of data, the need to protect against breaches, and the reporting of breaches that are done through either malice on the part of, say, a disgruntled employee or are the result of a hacker or something of that nature.

I'm going to ask about certain kinds of privacy issues around information that is very deliberately shared or made public, and that's people's tax filings and the public record in family law. Concerns have been raised about privacy and even the potential for identity theft through tax filings and information that is included as part of proceedings in family law.

Can either of you comment on how to deal with privacy issues in areas that for due process require public information to be available?

Mr. Vincent Gogolek: We did a submission to the Provincial Court of British Columbia on the availability online of non-conviction information, which is not exactly the question you're asking, and I would refer you to that to a certain extent.

There's also something called “practical obscurity”, where information is not widely disseminated. It's not available online, but it's still available if somebody wants to go and get it. Of course, we do have an open courts doctrine. The courts are supposed to be open, and judges do have control over their proceedings. If there is an appropriate case, then one party or another can apply to have information stricken that goes before the judge, who then decides. There are some mechanisms in place to deal with that, if there is some serious risk in the court at the time.

Mr. Michael Karanicolas: I haven't studied that issue specifically, but I will say that I would be interested to know if there are documented cases of identity theft that has occurred as a result or if it's just a flag that's been raised.

Mr. Pat Kelly: If, as part of the public record, the family law proceedings required the disclosure of a tax record, then there would be information contained in there that would be useful for somebody who wanted to commit identity theft. Even in the absence of a tax record, many types of family law cases would contain all kinds of information that could be put to malicious use when combined with information from other sources.

I'll share the rest of my time with Matt.

Mr. Matt Jeneroux: How kind.

Mr. Gogolek, you mentioned during your presentation the requirement for domestic data storage and what the province is doing. Could you elaborate a bit on that? I don't think we've heard yet at this committee what you guys are doing in the province.

Mr. Vincent Gogolek: It's something that has been in effect since the early 2000s. It was brought in, and there was very extensive debate. The Privacy Commissioner of British Columbia at the time, David Loukidelis, did a very extensive report. We did submissions, and a number of other people were involved. This was the outsourcing of what's called MSP, the provincial pharmacare plan information.

We have no opinion one way or the other on whether that should be done by government. It can be done by us, but the question is, what happens to the information? This was happening at the time the Patriot Act was being introduced after 9/11, and there was a great deal of concern over what would happen to very sensitive personal information that would be managed by an American company.

As a result, the government brought in extensive domestic data storage requirements in the B.C. Freedom of Information and Protection of Privacy Act, section 30.1. I would refer you to that for the background on that issue. It has worked well, and during the last review of our public sector act, which was held earlier this year, the commissioner, our organization, and the B.C. government all agreed that this is a good thing. It's popular with British Columbians, and it should be kept.

● (1210)

The Chair: Okay.

Mr. Vincent Gogolek: We just raised this as something that is not in the federal act, and we offer the example of B.C. for your consideration.

The Chair: I appreciate that very much.

We now move to the last questioner in the five-minute round, Mr. Bratina. Then we'll go to Mr. Blaikie, and then if anybody else has any questions that they'd like to ask, please let me know.

Mr. Bob Bratina (Hamilton East—Stoney Creek, Lib.): In recommendation 13, the commissioner suggests discretion be given to discontinue frivolous and vexatious complaints in specified circumstances. The Privacy Commissioner does not now have the authority to refuse or discontinue. Do you have a comment on that, Mr. Gogolek?

Mr. Vincent Gogolek: Yes. We're in favour of this change for reasons of judicial economy and to avoid wasting public resources.

We note that the Privacy Commissioner is saying that it should be held in his hands. You may remember that when we appeared on the Access to Information Act, our view was that the Information Commissioner should have that power, but the recommendation was that it be left with the departments.

We want to emphasize that we think it should be very tightly circumscribed, because we're talking about people's rights to complain. It should only be used in situations where the Commissioner is of the view that the complaint is frivolous, vexatious, or in bad faith. There should, of course, be the ability to appeal that decision.

Mr. Bob Bratina: With reference to your B.C. experience, the Public Sector Act has a domestic data storage requirement. Can we apply the way you do things in B.C. to federal procedures?

Mr. Vincent Gogolek: Yes. We have our section 30.1. A great deal of discussion that went on is available online from the commissioner's website. The former commissioner did a very extensive report. We did a report. There's been discussion of it during the two legislative reviews that have taken place since.

Not everybody is in favour of it. There are some public bodies that say, “This costs us money” or “All the cool kids to get to use this, so how come we can't?” However, the public consensus seems to be that this is a good thing. It's popular with British Columbians. The government brought it in specifically because of very wide public concern.

Mr. Bob Bratina: Was it you who mentioned the compensation paid to Mr. Bruyea?

Mr. Vincent Gogolek: Yes, Sean Bruyea.

Mr. Bob Bratina: What was the compensation about?

Mr. Vincent Gogolek: Well, he brought an action for damages under the Charter of Rights and Freedoms because of a violation of his charter rights. This was as a result of the repeated accessing and use of his very sensitive personal information. When you get our written submission, there's a link to his statement of claim, which was, as these things go, settled. He was paid an unknown amount of money, and nobody says anything after that.

That was settled, so there wasn't actually a decision at any point, but he was compensated to some extent. Our view is that people shouldn't have to be bringing court charter cases. There should be various remedies, which the commissioner has talked about in his recommendations.

● (1215)

The Chair: You have a minute and a half.

Mr. Bob Bratina: Does it say anything about the harm that was done? Quite a lot of the harm in cases like this could be issues of an elected official's integrity, and so on.

I'm not sure how we would come up with a regime of sanctions or damages.

Mr. Vincent Gogolek: We talked about this earlier in the context of the Access to Information Act.

There are quasi-criminal penalties for interfering with access rights. What needs to happen is some sort of sanction so that people treat these as actual rights and not as helpful suggestions that you really shouldn't do this. No. It should be that if you do this, you will have major personal, financial, or carceral problems. Also, people whose rights have been violated should be provided with a remedy.

Mr. Bob Bratina: Thank you very much.

The Chair: Now let's go to our last official round of questioning with Mr. Blaikie, and then, colleagues, let me know if you have any follow-up questions for Mr. Lightbound.

Mr. Daniel Blaikie: I want to follow up, Mr. Gogolek, on Mr. Kelly's question earlier about algorithms.

Am I right that the concern around privacy is less about revealing the algorithm itself and more the private information—the inputs, if you will?

Mr. Vincent Gogolek: It's a combination of things. It's what information is being collected and what it's for. This is one of the problems with data mining. It's one thing to mine data, but in some cases what you end up with is data strip mining and all kinds of information being put into the hopper.

Mr. Daniel Blaikie: To use your example of, say, an algorithm being used to determine people's candidacy for government training programs, is it your concern that an individual Canadian should be able to find out what personal information was used by whatever the algorithm is—not necessarily revealing what the algorithm is in itself, but to be able to ask what the inputs were, what personal information you had, and what you put into this black box? Is that what Canadians should have a right to know? Is that the contention?

Mr. Vincent Gogolek: Yes, for two reasons. One is the privacy of personal information. I gave you this information for this purpose, and now you're using it for that purpose, and I don't really see how it's connected. The algorithms are amazing. It's amazing what they come up with. Mr. Kelly is probably very familiar with what things come up in terms of credit. Some of it is astounding.

On one level, it's the collection and use for different purposes, and this is also where the information sharing agreements recommendation comes in in terms of mixing and matching all this stuff. We need to know generally how that's happening. That recommendation would provide a level of protection.

It's also about the proper functioning of government and in a way, I guess, about the proper functioning of quasi-judicial decision-making. If a public body makes a decision about your eligibility for training and they say no, you should have some ability to figure out why not.

Mr. Daniel Blaikie: It's more than just having a right to know what the inputs were in terms of personal information. It's also the details of the algorithm that—

Mr. Vincent Gogolek: Yes. What buttons are on the blender: frappé, purée, goo-ify, whatever? You might not have to know exactly where all the wires are connected in a blender, but you need to know that, yes, this was run through a blender, here are the buttons, and here's what went into the blender.

Mr. Daniel Blaikie: I don't know if this is a real concern—it's certainly speculative on my part—but a lot of those algorithms wouldn't be developed in-house by government, it seems to me. A lot of that is farmed out to private companies. Do you think if those algorithms were being revealed under the Privacy Act, there would be an issue of government being able to access the services of companies that are very good at doing that because they don't want to reveal to competitors the nuts and bolts of what they do?

● (1220)

Mr. Vincent Gogolek: In our experience, companies that have the black boxes absolutely do not want anybody to know anything about it. A lot of times they're in a competitive situation and that's understandable, but I think there's a difference between knowing exactly how you make the box actually work and knowing what goes in and generally what the buttons are on the blender.

Mr. Daniel Blaikie: From a legislative view, how do you think we should be thinking about that problem to strike that right balance between giving Canadians enough information about how decisions are being made in this fashion without unduly disadvantaging government, if you will, from accessing the best services in that industry to create that decision-making software?

Mr. Vincent Gogolek: Part of it is that the government has a lot of purchasing power. A lot of companies want to sell to government. Their contracts are subject to freedom of information legislation. If they were dealing with another company, that would not be an issue for them. Some companies may not want to bid on federal contracts because they're concerned about the level of disclosure they would have to provide on the workings or the methodology of the black box—i.e. “here are the blueprints, here are the circuit boards, and here's the way we make it do what it does,” as opposed to “we take these things, put them together, and the smoothie comes out”.

The Chair: Mr. Blaikie, if you have some more follow-ups, we'd be glad to get you back on the list.

I'll chime in here for just one little piece.

Sometimes when you get hold of the blender, you can take it apart and see how it's engineered. These are things you have to be careful of. As a former software developer, protecting things like code and so on are very important for a firm's competitiveness.

Mr. Lightbound is next.

[*Translation*]

Mr. Joël Lightbound: Thank you.

I'd like to come back to what I was saying earlier.

Mr. Karanicolas, you talked about a loophole in terms of the information sharing that goes on with partners like the Five Eyes alliance. Do you think it's possible to close the loophole using the Privacy Act somehow, in order to protect Canadians, or is the problem beyond the scope of the act?

[*English*]

Mr. Michael Karanicolas: We support as necessary first steps the Privacy Commissioner's recommendations that information sharing agreements must be in writing, must be clearly specified, and must be sharing information for specific purposes. We think those agreements should also be public so that there can be a better debate on how information sharing takes place and Canadians can get a better understanding.

You know, I learned more about Canada's information sharing systems from Edward Snowden and those disclosures than I did from studying the system myself. I think that's a problematic situation.

[*Translation*]

Mr. Joël Lightbound: I have another question for you.

I'd like you to talk to us about the exceptions that allow institutions to share information with one another.

The exception in section 8(2)(b) permits a government institution to disclose information under its control “for any purpose in accordance with any Act of Parliament or any regulation made thereunder that authorizes its disclosure”.

For instance, Bill C-51 states that the sharing of information must comply with the Privacy Act. The Privacy Act, however, authorizes the sharing of information provided that it complies with another act or other regulations. It's a bit like trying to fit a square peg in a round hole.

I'd like to hear your thoughts on that exception, which, in my view, basically renders the Privacy Act inferior to other regulations and acts.

Mr. Karanicolas, you can go first.

[*English*]

Mr. Michael Karanicolas: I need to defer to my colleague on this aspect because my presentation on Bill C-51 is tomorrow and I haven't prepped that yet.

Mr. Vincent Gogolek: We presented yesterday, so I guess we're —

Mr. Joël Lightbound: That's convenient.

Bill C-51 says the sharing of information must comply with the Privacy Act. Everything that's under it must comply with the Privacy Act, but when you look at paragraph 8(2)(b) in the Privacy Act, it says that information sharing is authorized—

● (1225)

Mr. Vincent Gogolek: It's authorized by any law.

Mr. Joël Lightbound: —provided that it's regulated or it's authorized by another regulation. It's authorized by Bill C-51. Then Bill C-51 says, “We respect the Privacy Act”, but then the Privacy Act says it's authorized if any other regulation authorizes it.

Mr. Vincent Gogolek: It is confusing, and I think the government itself is confused, because in its backgrounder to the green paper on national security and Bill C-51, it talks about that very problem. At one point it says that because the act authorized disclosure, it satisfies paragraph 8(2)(b), which is the lawful authority exception, but the act says that it's subject to other acts that prohibit or restrict the disclosure of information.

You have two provisions that seem to contradict each other. Our view is that it is subject to the Privacy Act because of that statement in the Security of Canada Information Sharing Act that says it is subject to acts and regulations that provide those protections.

It's not an easy question, and that is why it's important to improve the Privacy Act as much as possible.

Mr. Joël Lightbound: I invoked Bill C-51 just by way of example, but I was wondering if you had general thoughts about paragraph 8(2)(b) as an exception to information sharing.

Mr. Michael Karanicolas: I can say as well that these paramountcy clauses tend to be a bit problematic. They are problematic in the Privacy Act, and they're also problematic when we find them in the Access to Information Act.

Generally speaking, when we have a piece of legislation that's supposed to set out standards, it creates tension when you say “Here are the standards by which the government is going to operate, except for any other law that contradicts it.”

If you're going to consolidate the standards, it makes more sense to either not have those kinds of exceptions or to say that if other laws want to impact or want to disclose information, it must be done according to the standards set out in this law. That's the solution we propose for the Access to Information Act, and the same is true for the Privacy Act.

Mr. Joël Lightbound: Might I ask another question?

The Chair: By all means, yes.

Mr. Joël Lightbound: We had Chantal Bernier here, who said that for information sent to this committee, information sharing should not simply be based on the necessity of other programs or other governmental activities, but it should also be evaluated against the Charter of Rights and Freedoms. I was wondering if you had an opinion on this suggestion and what impacts you think it could have.

Mr. Michael Karanicolas: There's a reason I started my presentation by talking about privacy as a human right.

The fundamental duty of government is to safeguard and protect the human rights of its people, and that includes providing security, of course, and it includes guaranteeing freedom of expression, but it also means respecting their privacy. Going back to the Information Commissioner's recommendation, I do think that the discussion of privacy impact assessments and mandating those is a good step along that path. That should always be a concern when you have legislation or policies that are affecting privacy. The rights aspect should be central to considerations.

Mr. Joël Lightbound: Mr. Gogolek, would you comment?

Mr. Vincent Gogolek: I don't disagree with Madam Bernier, but I think that including the necessity in the act itself works along the same lines as the Oakes test for proportionality. It has that aspect to it, because that's the way we generally interpret things.

Mr. Joël Lightbound: Can I have one last question, Mr. Chair?

The Chair: Sure.

Mr. Joël Lightbound: Thank you.

My last question would be regarding metadata. It is not defined anywhere in Canadian legislation. Do you think the Privacy Act would be a good statute where we could start to define metadata and its use by government?

Mr. Michael Karanicolas: Sure. I think there's a risk that it will bump a little bit into what my colleague mentioned before about having acts written in a technologically neutral fashion. Metadata means one thing today; it could well mean a totally different thing in five or 10 years.

I do think that metadata has a very high privacy value. Its disclosure and its sharing can have very high risks associated with it. It can be extremely personal, and I think that it needs to be strongly protected.

● (1230)

Mr. Vincent Gogolek: I think the Spencer case provided a very good guideline to us in terms of the importance of metadata and in terms of it being personal information that is protected.

I know that some parts of the law enforcement and security communities would rather Spencer had been decided a different way, but that's what the Supreme Court of Canada had to say about metadata, that there is an interest in it. I think that a lot of the way they've been doing business was based on their interpretation: “Oh, this is phone book information. This is tombstone information.” Well, no, it's not; it's personal information, and a lot of it can be very sensitive.

The Privacy Commissioner actually did a very good piece contradicting that in setting out how metadata is personal information.

I was going to mention the concern about being too specific in the actual legislation itself.

The Chair: Mr. Saini, do you have a quick follow-up?

Mr. Raj Saini: I'm sorry to pick on you, Mr. Karanicolas, but Mr. Gogolek stole all my answers during his remarks.

You raised something when you were answering another question, and that prompted me to ask this question.

In terms of business people, for example, in Canada they divulge to the CRA whatever they need to. That information, especially if a business person here has foreign subsidiaries or foreign interests, may be shared with a country that we have a transaction agreement with.

What happens if a third country has a transaction agreement with the second country, but we don't have any agreement with that country? How does that work, then? That information, especially because it's information regarding a corporation, could have certain intellectual property involved. Certain information can be gleaned from a tax return. I'm just wondering how that works. How do we prevent the information of a Canadian citizen from going to a country we don't have an agreement with but another country may have an agreement with?

Mr. Michael Karanicolas: I think this strays a little bit outside my expertise, but generally speaking, you would want to see information sharing agreements specify clearly how the information may be used, and that includes further disclosure. This is a major issue both in the public sector and in the private sector.

I have my contractual relationships with Facebook and Twitter. I give them information about me. They have licence to share that information with third parties that I don't interact with. I don't know what their names are. This is a major concern.

Generally speaking, from the government's perspective, I would think that should be spelled out in a co-operative relationship with the other governments, the other agencies. If they're found to be breaching that relationship, if they're not playing by the rules that have been established, then the government should consider terminating that engagement.

Mr. Raj Saini: You mentioned remedy in your opening remarks. If there is a data breach, let's say, in a second or third country, how would that work? You have a specific set of laws here and you have specific penalties here. If the data breach happens or something happens in the second or tertiary country, their laws or their fines may not be as severe as they are here. If somebody here has a data breach of their information in another country, how would you...?

Mr. Michael Karanicolas: This is the problem with global data flows. We're used to traditional ideas of jurisdiction. Even international law is based on this idea of where a country ends. When you have information that's flowing all over the place—when you have the Internet, which doesn't have traditional borders—it's very difficult to apply traditional understandings of jurisdiction and traditional protections of rights.

This is one of the reasons we supported the Information Commissioner's recommendation to engage more with colleagues. It's good to try to push for common approaches to privacy and common approaches to human rights protections, and certainly with the countries we roughly see eye to eye with in terms of how human rights should be protected.

I brought up the example of the Ashley Madison user in Saudi Arabia or Russia whose information was suddenly disclosed and is now personally under threat. We would want to see the Canadian government and Canadian regulators taking action in those kinds of cases, but if it happens the other way around, it's difficult to say. This is why international collaboration is so important. Right now I don't think there are clear rules for how that should be addressed.

● (1235)

The Chair: Go ahead, Mr. Blaikie.

Mr. Daniel Blaikie: I want to go back to Mr. Lightbound's question about the necessity testing being tied to the charter as opposed to the federal program. I'm looking for just a little more education, maybe.

It seems to me that tying into the charter would be less restrictive than tying into the program, because federal programs and collection of information would be.... You could make a charter challenge if you felt for some reason that the government was, for the purposes of a program, collecting information that violated your charter rights, information that they didn't have a right to have or a right to collect. That would be something for the courts to determine. Having a further necessity test that's tied to the purposes of the program is actually a restriction within that larger restriction.

Isn't that how it works? If someone felt that the government was violating their charter rights by collecting information in a certain way, they could take that to court, and having the necessity test tied to the federal program would be a restriction within that—or do I just not understand how those two things interact?

Mr. Vincent Gogolek: There are independent remedies in the charter for a breach, and of course we have privacy rights in the charter in sections 7 and 8. That would be independent of anything to do with the actual Privacy Act itself in terms of something being necessary.

When you have a charter breach or after you find a breach, you look at section 1 in terms of whether it is justified, because rights are not infinite and uncontradictable. There may be very good reasons for it. There is something called the Oakes test, which deals with proportionality, necessity, and linking to the purposes of that breach. That's very well-defined constitutional law.

Mr. Daniel Blaikie: Here's what I'm trying to understand. Let's say we're applying to a government program to receive a drug of some kind in order to help with therapy. A necessity test tied to the program might ask about my employment history, which really isn't relevant to that. Because of the necessity test that's tied to the program, you wouldn't have a right to ask about my employment history. When it's a health-related issue, you may be able to ask certain health-related questions and I would have to disclose the information in order to access that program, but I don't see how the charter piece actually is more restrictive than that. To me, that seems to rule out far more things than the charter provision.

Maybe there is just something in this I'm not understanding.

Mr. Michael Karanicolas: You can create a legal standard that goes beyond the charter protections. The charter is the point at which rights must be respected, and you can take a legal standard that goes beyond that.

In terms of the actual formulas for remedy, though, in that kind of case you would complain to the Privacy Commissioner either way, whether you were relying on a constitutional provision—

Mr. Daniel Blaikie: Really what I'm asking about is that I just don't understand tying the necessity test to the charter itself, which is already there and in effect is more restrictive than having one tied to the nature of the program and the information that would be required for a specific program. That, to me, seems to be more restrictive than a more general one; as long as it doesn't violate my charter rights, then the government can ask for that information.

Do you see what I mean? This necessity test for the charter is being pitched as more restrictive. I just don't understand how it would actually be more restrictive than saying, “You are restricted to asking only for information that pertains to your needs in order to be able to deliver this program.” That, to me, seems actually to be the more restrictive test. Is there something I'm not understanding? How does the charter, generally speaking, get more restrictive than something that would be tied to asking for information that pertains only to what you would need in order to deliver the program?

● (1240)

Mr. Vincent Gogolek: The charter is more overarching. I'm a little reluctant to try to interpret somebody else's argument that I just saw in terms of the transcript, having read it once. I thought it was interesting, but I would really have to take a look at it. I can speak to our experience in B.C., where we do have a necessity test, and it does work.

In terms of the Privacy Act being brought up to the standard that would be expected of modern privacy law, I think that putting it in, in the way the commissioner recommended, is probably the way to go.

The Chair: Thank you very much, colleagues.

I thank our witnesses for coming in today.

Thank you, Mr. Gogolek, for appearing again, and thank you, Mr. Karanicolas, for your personal first appearance on behalf of your organization, the CLD.

I expect that we'll have an opportunity to call you or your organizations back again at some particular point time as we review other legislation that's relevant and germane to this committee's business. We thank you very much for your time.

Colleagues, I have some things that I need to discuss with you. They involve the availability of witnesses whom we've asked to come before the committee on a study unrelated to this one. I would like to protect the personal information of some of these witnesses, so I would love to entertain a motion to go in camera.

A voice: I so move.

(Motion agreed to)

The Chair: We'll suspend for a second to go in camera. Let's get back to work as soon as possible. We only have a few minutes. Thanks.

[*Proceedings continue in camera*]