HOUSE OF COMMONS
CHAMBRE DES COMMUNES
CANADA

Standing Committee on Access to Information, Privacy and Ethics

ETHI • NUMBER 024 • 1st SESSION • 42nd PARLIAMENT

EVIDENCE

Tuesday, September 27, 2016

Chair

Mr. Blaine Calkins

Standing Committee on Access to Information, Privacy and Ethics

Tuesday, September 27, 2016

● (1100)

[*English*]

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

Good morning, everyone.

This is our 24th meeting of the committee. This is our third or fourth meeting on our study of the Privacy Act. We are thrilled to have some high-calibre witnesses with us again today.

We have Colin Bennett, professor with the department of political science at the University of Victoria, and Michel Drapeau, professor with the faculty of common law at the University of Ottawa, who is no stranger to testimony here on the Hill.

From the Canadian Bar Association, we have Gary Dickson and Kellie Krake.

Welcome to all. We cannot wait to hear what you have to say. We'll have 10 minutes from each organization or individual. We have simultaneous translation, so I ask that you speak slowly, clearly, and articulately in order to have simultaneous translation.

We'll begin with you, Mr. Bennett, for up to 10 minutes, please.

Professor Colin Bennett (Professor, Department of Political Science, University of Victoria, As an Individual): Thank you very much, Mr. Chairman. I'm pleased to be here.

I am a professor of political science at the University of Victoria. I'm currently on sabbatical leave at the University of Toronto, so I haven't come all the way from Victoria today.

I have written or edited a number of books on the subject of privacy protection, both comparatively and historically, and that's my expertise. I'm generally known for my comparative work on privacy governance in both the public and the private sectors.

I'd like to begin by saying something about the history of the Privacy Act and why it came into being, because I think that historical context is important.

At the time the act was passed, Canada was only one of a handful of countries, most of which were in Europe, that had passed any form of privacy protection legislation. It was enacted with little public media or parliamentary debate. To a large extent, it was motivated by the associated passage of the Access to Information Act and the need to ensure that both acts were compatible with respect to exemptions.

The title is a misnomer. The law addresses just a subset of the multiple issues and concerns embraced by the word “privacy”. It's more properly regarded as a data protection statute. That's the word that's typically used in Europe to cover the regulation of the collection, processing, storage, and disclosure of personally identifiable information.

As the Privacy Commissioner and many others have pointed out, the Privacy Act is in dire need of modernization. It is a first-generation statute, and two or three other generations have evolved since. The lack of reform has also meant that a good deal of the content of the regulation is contained in an accumulation of Treasury Board Secretariat guidance that can sometimes be ignored or selectively interpreted.

The act is also based, in my view, on the dated assumption that government information is contained in neat data banks and can be listed, managed, and regulated. It's also based on the false assumption that the chief threat to privacy came from state bureaucracy rather than from the private sector. There are now over 100 countries in the world that have some form of comprehensive data protection law, and virtually all of them cover the practices of both corporations and government.

Given our complex federal system, that was never going to be an option for Canada. We are stuck with some legacies that are difficult to escape from. In my view, the general task here is to amend the law in such a way that the basic privacy principles remain intact, which embraces the more contemporary ideas about how to protect personal data in a networked environment in which personal data can be shared instantaneously and easily between and within organizations. The main difference between the laws that were passed in the 1980s and the 1990s and those that were passed in the 21st century is that contemporary law now embraces a full range of different tools or instruments for privacy.

I am in general agreement with what the Privacy Commissioner said to you in his submission of March of this year. I do not disagree with any of the suggestions that he made, but I would like to focus in the time remaining on four areas of reform mentioned in his submission: data breach reporting, privacy impact assessments, the overall powers of the Privacy Commissioner, and the question of information sharing.

I also have some final comments on the capture of personal data by federal political parties. I know this was something you've asked witnesses about in your previous sessions. I have written about that extensively. I've researched it and I want to make a few comments about it.

First, with regard to data breach reporting, the frequency of data breaches in the federal government is quite striking. Data breaches cost money and they damage trust and reputation. Mandatory privacy data breach notification is now a feature of modern data protection law. It's now required under some conditions for Canada's private sector under the amendments to PIPEDA.

It's also crucial, in my view, to combine the stick of mandatory data breach reporting with a carrot that says that if you've taken proper technical measures and safeguards to protect that data through encryption, then it's not that you get out of jail free, but you just have to do less in terms of reporting.

● (1105)

Organizations and agencies need to be incentivized to encrypt data. Therefore, I would strongly suggest that any mandatory data breach reporting requirement be accompanied by appropriate legislative requirements for physical, organizational, and technical safeguards similar to those that are found in PIPEDA.

Second, privacy impact assessments, or PIAs, have been a feature of the privacy protection landscape since the late 1990s, and Canada was one of the first countries to think seriously about this issue and their appropriate role. Ideally, they should be a recurrent process, an ongoing process, rather than just a checklist. They're designed to be an early warning, and they're particularly critical when programs and services that have potentially significant implications for privacy are being contemplated or amended. Experience suggests, however, that they are more likely to be effective when they're embodied in existing administrative procedures, such as technology procurement, budgetary submissions, and so on.

The OPC has reported that the quality of PIAs in the federal government is very uneven because there's no legislative requirement to conduct them, as there is in other countries and in some provinces. I therefore strongly support the OPC's recommendation that the current TBS guidance be given statutory force.

Thirdl, with regard to the powers of the Privacy Commissioner, when the Privacy Act was passed, there was little contemplation that the commissioner would be anything more than a standard ombudsman within the general parliamentary tradition, and an awful lot of the text of the Privacy Act is about the complaints investigation process. That is extremely important.

One take-away I'd like to give to you here is that comparatively, through my experience and research, the most important powers of a privacy commission are those that are proactive and general or systemic, rather than those that are reactive or individual-based. I would like to see the act reformed in such a way that some of the more proactive powers are included in the legislation. That includes order-making power. The commissioner can only make non-binding recommendations; he cannot compel a public body to take or cease any action without recourse to the courts.

I know there's been a lot of debate about this point over the years. I am encouraged that the Privacy Commissioner has now come around to the view that he does require order-making power such as that exercised by the commissioners in B.C. and Alberta. I think it's a natural progression.

The commissioner should obviously be given an explicit public education and research mandate, the same as that provided under PIPEDA. He does that anyway. It's not in the law. It shouldn't be controversial. A government agency should also be given the requirement to consult with him on draft legislation and regulation with privacy implications before they're tabled. He suggested that. It's a natural thing to do. It shouldn't be controversial.

Finally, on information sharing, the Privacy Act, in my view, has been ineffective in regulating the sharing of personal information among government agencies. I say more about this in my testimony. I won't go into any great depth here. The OPC has recommended that any sharing of information among agencies be made in a written manner. The problem, in my view, is the so-called “consistent use” exemption, which was originally intended as an exceptional circumstance—just those exceptional circumstances when agencies need to share data when they didn't think about it and it wasn't included in the Info Source database.

If you look at Info Source now, you see a whole range of consistent uses that are listed. I think it's got out of control and I think it needs to be reined in. There should be written requirements, and so on.

Finally, if I may, I'd like to say something about the capture and processing of personal data by federal political parties. I understand that the committee has been interested in this question. I'd be interested in answering any questions you have about it. I wrote a report on this subject for the Office of the Privacy Commissioner back in 2012, and I actually testified before this committee two or three years ago when you were interested in social media and social networking in relation to this subject.

● (1110)

Political parties are largely exempt from Canadian privacy laws. They're not covered under PIPEDA or substantially similar provincial laws, with the exception of the Personal Information Protection Act in B.C. They're not government agencies, they're not covered by the Privacy Act, and they're largely exempt from CASL, the spam legislation, as well as from the do-not-call regulations administered by CRTC.

Thus, for the most part, individuals have no legal rights to learn what information is contained in party databases, which are extensive; to access and to correct those data; to remove themselves from the systems; or to restrict the collection, use, and disclosure of their personal data. For the most part, parties have no legal obligations to keep that information secure, to only retain it for as long as necessary, or to control who has access to it.

I am not arguing that the Privacy Act is the appropriate statutory vehicle to deal with this problem, and there are also problems with bringing parties under PIPEDA, but as I've done a lot of research on this subject, I just want to alert you to the fact that this is a huge gap in the Canadian privacy regime, and, in my view, and that it requires some urgent resolution.

I'll leave it at that for now. Thank you very much for your attention. I look forward to your questions and I hope to submit a longer submission later in the process.

● (1115)

The Chair: Thank you, Mr. Bennett.

Go ahead, Mr. Drapeau, please.

Colonel (Retired) Michel Drapeau (Professor, University of Ottawa, Faculty of Common Law, As an Individual): Mr. Chair, ladies and gentlemen, thank you for giving me the opportunity to comment on the proposal advanced by the Privacy Commissioner in his letters of March 22 and September 13.

For reasons of brevity, and I will be brief, permit me to identify the recommendations with which I agree, without commenting on any of them.

I agree in principle with 11 of the recommendations made by the Privacy Commissioner, the OPC, namely recommendations 1 to 4, 6 to 8, and 11, 12, 14, and 16.

However, I disagree with six of his recommendations. Let me touch very briefly on the reasons for not endorsing these in my further comments.

First is recommendation 5, which deals with expanding judicial recourse and remedies under section 41. The only reason for my disagreement with this recommendation is that it doesn't go far enough. I believe one of the most important remedies that can be provided to a complainant is to handle his or her complaint in a reasonable amount of time. This is currently not happening. I recommend that a time limit be imposed upon the OPC to make findings and recommendations.

Recommendation 9 is to provide the OPC with an explicit public education and research mandate. I disagree with this. The Privacy Act has been in existence for 33 years. It's not a complex piece of legislation. Its breadth and its reach are rather limited. It deals exclusively with personal information in records under the control of the federal government. I don't believe the public needs to be educated on this right of access to their personal information. I anticipate that such an added function would lead to a substantial increase to an already large bureaucracy at the OPC.

I'm also of the mind that the role of public education and research, if required, should be left to the universities and research organizations or bar associations.

Recommendation 10 is for a five-year review of the act. I also do not believe there is a need for review on such a relatively frequent basis. I'll go along with 10 years, but certainly not five years.

Recommendation 13 is to grant the OPC the discretion to discontinue or decline complaints in specific circumstances. Under the Privacy Act, Canadians have a quasi-constitutional right to access their personal information and to complain to the OPC if they feel that their rights have been violated. I feel it would be wrong to empower the commissioner with the discretion to refuse to investigate a complaint, as it would disenfranchise the complainant and deprive him or her of any possible remedy before the court.

Recommendation 15 is to extend the coverage of the act. The commissioner recommends extending the right of access to foreign nationals. I disagree, at least for now.

At present, the OPC is one of the slowest complaint tribunals in Canada. As a case in point, I have a complaint at the moment that has been outstanding since June 2012. We have been informed recently that we shouldn't expect findings before December of this year. It took four years. I will admit it is a very complex case, but it took four years to get to it.

If you look at their report from last year—this year's report will be tabled sometime today—we know there is a one-year backlog already. Anybody submitting a complaint today has to wait at least a year if they were to be at the front of the queue from this time onward. I submit that it would be folly to extend coverage of the act to foreign nationals until we can provide Canadians with the service they deserve.

I must now address the fact in his September 13 letter, the commissioner has repudiated the recommendation he made six months earlier.

● (1120)

I have already indicated my agreement with the recommendation on March 22 by which he proposed a hybrid system for the investigation of complaints. I agree with that. However, I strongly disagree with his September letter, in which he now asks for order-making powers.

[*Translation*]

I have trouble understanding why the commissioner has done an about-face and is now requesting order-making powers rather than the hybrid model. Like him, I will refer to the La Forest judgment. Justice La Forest warned us that such a change would be costly, that it could further delay the investigation process and, worse still, that it could lead to closed-door hearings.

I will now quote Justice La Forest's statements that are included in the Privacy Commissioner's letter.

> There is a danger that a quasi-judicial, order making-model could become too formalized, resulting in a process that is nearly as expensive and time-consuming as court proceedings. It is also arguable that the absence of an order-making power allows the conventional ombudsman to adopt a stronger posture in relation to government than a quasi-judicial decision-maker. There is also some virtue in having contentious access and privacy issues settled by the courts, where proceedings are generally open to the public.

Thank you for your attention.

[*English*]

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

We now move to Mr. Dixon on behalf of the Bar Association, for 10 minutes, or is it Ms....?

Ms. Kellie Krake (Staff Lawyer, Law Reform, Canadian Bar Association): Thank you very much for the invitation to present the CBA's views on the Privacy Act amendments.

The CBA is a national association of 36,000 lawyers, law students, notaries, and academics. An important aspect of the CBA's mandate is to seek improvements in the law and the administration of justice. It's that perspective that brings us before you today.

Our submission on the Privacy Act amendments was prepared by the Canadian Bar Association's privacy and access law section. With me today is Gary Dickson, an executive member of that section. He served as Saskatchewan's first full-time information and privacy commissioner for 10 years. He also served as an elected member of the Legislative Assembly of Alberta for nine years, with specific responsibility for access to information and privacy legislation.

Mr. Dickson will now address the substance of our submission and respond to any of your questions.

Mr. Gary Dickson (Executive Member, Privacy and Access Law Section, Canadian Bar Association): Good morning, Mr. Chairman and members.

You will have already seen the Canadian Bar Association's written submission in response to each of the 16 suggestions from the Privacy Commissioner, at least as they stood when he wrote to your committee on March 22.

The position of the Canadian Bar Association is, and has been, that this 1983 statute is long overdue for reform. More than 200 government institutions are currently subject to the Privacy Act , and collectively they collect, use, and disclose massive volumes of personal information of Canadians. The CBA is supportive of 13 of those recommendations. Let me highlight our thoughts on three of the recommendations that the CBA did not fully agree with.

Recommendation 6 may be the most significant, in that it deals with the role and powers of the Privacy Commissioner. The CBA completely agrees with the commissioner that the current model of pure ombudsman requires reform. This, of course, confers on the Privacy Commissioner broad powers to undertake investigations, but at the end of the day only the limited power to offer recommendations, which may be accepted in whole or in part or rejected. This is a model that's currently seen in Yukon, the Northwest Territories, Nunavut, Saskatchewan, Manitoba, Nova Scotia, and New Brunswick.

If the committee agrees that change is needed, there are essentially two models that exist in other Canadian jurisdictions to consider for this important office. One is the order-making model, under which the Privacy Commissioner is in effect an administrative tribunal and can issue enforceable orders to government institutions. This is the model that exists in British Columbia, Alberta, Ontario, Quebec, and Prince Edward Island.

The alternative we suggest would be the newer model that's been created and then implemented in Newfoundland and Labrador's June 2015 amendments to their access and privacy law. In our paper, at page 8, we describe this as the enhanced ombudsman model.

I know this committee has had the opportunity to hear from the authors of the seminal report that was done in Newfoundland that had been shared by Clyde Wells and is aware of the reasons for the recommendations. The preference of the CBA, when we looked at the two models initially, was that the enhanced ombudsman model would be the preference.

Mindful that the Privacy Commissioner has just revised his position and moved from supporting the enhanced ombudsman model to the order-making model, we thought it might be useful for the CBA to offer a thumbnail sketch of some of the advantages and disadvantages that we've identified with the two different models.

With the order-making model, an advantage is that it would clearly align more closely with international models of data protection. That's what you would see in the Federal Trade Commission and the Federal Communications Commission in the U.S., as well as in the United Kingdom and Mexico. Most European data protection authorities also have that kind of an order-making tribunal model.

Clearly we would see much a more timely response to the oversight office once formal investigations are started. In the experience in those provinces that have order-making, there tends to be a more positive response and a more timely response when the commissioner comes calling. Obviously there would be higher levels of compliance in cases where the government institution would otherwise not accept a recommendation from the commissioner, although you've already heard from the Information Commissioner that most recommendations are now accepted without any order-making capacity.

With regard to the disadvantages, the process tends to be more formal and more attenuated when you have an administrative tribunal. The strict obligation to ensure procedural fairness typically builds in longer time periods to move a file forward. That could translate to even longer delays than those already encountered, and certainly less flexibility for the commissioner. The process will be less user friendly for your constituents and perhaps more intimidating to individuals who make complaints to the order-making commissioner. It will likely mean dividing staff and creating a separate group of intake officers and mediators, then a separate group of adjudicators or hearing officers, and then installing within the office some kind of a wall between the two groups.

● (1125)

The chief advantage of the enhanced ombudsman model is a less formal, more flexible process that we think will be more user-friendly for your constituents. Allowing the commissioner to hold government institutions to account and order them to provide relevant documents and responses within deadlines, which don't currently exist for the privacy commissioner under the Privacy Act, will go a long way towards expediting and accelerating the process. I remind you that this process is often prolonged and arduous, the key being how to get co-operation from government institutions in providing the documents and information you need. We think improved efficiency should flow from the new powers suggested to better control the process of an investigation.

On the substantive issue of whether there has been a breach, the enhanced ombudsman model shifts the onus to government institutions. This is something we think highly appropriate. If a government institution is dissatisfied with a decision of the commissioner, it's up to the government institution to go to court to obtain a final determination.

Finally, as we see it, it would be easier for the privacy commissioner's office to transition to the enhanced ombudsman model than to an order-making model. When I recently spoke with Newfoundland and Labrador's information and privacy commissioner's office, one of the senior officials commented that the new system, only a year old, was working in an excellent fashion. He thought it had been very successful.

The disadvantage is that we only have about a year of experience here. Newfoundland embarked on this new process in June of 2015, so it's a limited time. We understand, though, that the system appears to be working well at present.

One of the other items we had a concern with was recommendation 8, the prior consultation suggestion or requirement. We note that the Treasury Board policy on privacy protection, section 6.2.12, already requires notification of the commissioner of

> any planned initiatives (legislation, regulations, policies, programs) that could relate to the Act or to any of its provisions, or that may have an impact on the privacy of Canadians. This notification is to take place at a sufficiently early stage to permit the Commissioner to review and discuss the issues involved.

We don't know to what extent this is not being complied with, but it's quite clear and it's an appropriate direction.

We absolutely agree with the importance of early consultation, but we question whether it's realistic to make it a condition precedent to a bill's first reading. My experience as a House leader in the official opposition of a provincial legislature is that from time to time bills have to be introduced on short notice. It may be the end of a session or it may be that bills need to be introduced quickly, not to shorten and abridge the period for consideration but in fact to allow for ample consultation. In most cases it would be absolutely appropriate to have prior notice, but I can imagine cases in which it might not be useful or realistic to have a statutory requirement for prior notice.

On number 16, the personal information exemption, I can simply say that the CBA could not achieve a consensus position. This is one of those rare cases of a difference of opinion between the Information Commissioner and the Privacy Commissioner. We recognize that most provinces have this kind of two-part test, first determining whether it's a breach of personal information privacy and then considering whether it an unlawful or unreasonable invasion of privacy. We could not achieve a consensus position on this point. CBA represents a large number of lawyers with many different kinds of clients and views, and in this area we are not able to assist the committee in by offering a concrete suggestion or recommendation.

Thank you. I appreciate the time and the opportunity. The Canadian Bar Association looks forward to your questions.

● (1130)

The Chair: Thank you very much to our esteemed witnesses.

We're now going to proceed to a round of questions for the first four members of the committee.

Our first MP is Mr. Massé. Please go ahead.

[*Translation*]

Mr. Rémi Massé (Avignon—La Mitis—Matane—Matapédia, Lib.): Hello.

I would like to thank the witnesses for taking part in this important exercise.

I have a practical question for you. Clearly, we are concerned about protecting privacy in the context you are familiar with. The federal government is a huge organization, with many departments and agencies, and personal information is collected under many programs.

In this context, what practical steps can be taken to combine the need to protect privacy with the need to offer citizens services that are effective, less expensive and more modern, as a result of technology?

The question is open to all the witnesses.

Col Michel Drapeau: I think our public service is very well informed. It is well equipped to provide information and submissions, while bearing in mind privacy issues. This is not too onerous.

People know that some of their personal information is recorded in documents belonging to various departments. In my own experience, I have regular dealings with various government bodies. In exchanging correspondence or documents, everyone is aware of the need to apply the act as it stands.

Earlier I said that the act is not particularly complex. It really is not. You have to pay attention to certain nuances but, in practice, you know which parts of a document contain personal information. We have to rely on the good judgment of each public servant, who can consult experts if necessary to ask whether they can disclose that bundle of information.

● (1135)

[*English*]

Prof. Colin Bennett: Thank you for your question, and it's really a big question.

To deal with any privacy legislation, how do you strike the right balance between the rights of the individual and the legitimate service needs of government agencies?

The Privacy Act is based on a theory. It's based on a principle that when individuals give information to an organization, they do so for a specified, transparent, and confined purpose. That principle is under threat by the data processing activities of government and the private sector in the belief that in this era of big data analytics, you can take information from a variety of different silos, correlate it, and find correlations that are going to be of interest to government in the implementation of public policy.

The Privacy Act is based, as I said, on this dated assumption that information can be categorized and put in silos, put in data banks. I think that is under severe challenge. The Info Source tool is dated and reflects a reality that is 30 years out of date.

Finally, government can do an awful lot in making public policy and delivering services without personally identifiable information. In answer to your question, you should identify the information and anonymize the information in an appropriate way, so that you can have both worlds. This comes under the title of privacy by design, whereby you build privacy in at the beginning. Those are the kinds of tools that the Privacy Commissioner should have, and that should be made more explicit in the Privacy Act.

[*Translation*]

Mr. Rémi Massé: Thank you, Mr. Bennett.

Mr. Dickson, if I may, I have a supplementary question for Mr. Bennett relating to part of his answer to my question.

You said that creating a directory of personal information databases, which is called Info Source, could be a tremendous waste of time and energy. I would like to understand exactly what you mean. Do you have any concrete suggestions to improve this aspect of the requirements?

[*English*]

Prof. Colin Bennett: I hear from privacy professionals and from the Privacy Commissioner's office that it's generally not used a lot. It is often dated. It produces huge headaches for government departments that have to keep it up to date and define consistent uses.

I certainly see the value in having something like that when you are trying to regulate information sharing, but I do wonder sometimes whether or not it's a bureaucratic requirement that has outlived its necessity.

[*Translation*]

Mr. Rémi Massé: Mr. Dickson, you may answer.

[*English*]

Mr. Gary Dickson: Thank you for the opportunity to respond.

The question you asked is not much different from the question that would have been asked more than 30 years ago when legislators and parliamentarians were looking at trying to create a regime that would provide adequate protection for the privacy of Canadians, yet at the same time allow the necessary collection, use, and disclosure of personal information to keep people safe and to deliver services that your constituents and all Canadians require and expect.

There was a royal commission in Ontario in 1980 that produced a seven-volume report wrestling with that very question. We have certainly the experience of over 30 years with legislation.

I think the way we try to address and meet this constantly changing world of threats and challenges and so on to personal privacy is flexibility and comprehensive protection. For that you need legislation that's adequate to the task, which is the exercise you and your colleagues are currently engaged in. It means having a privacy oversight agency or, as Colin would say, a data protection agency, that has the necessary flexibility to be able to deal with changing threats and constantly changing new privacy-impacting technology.

The other thing that is always important to recognize is that it's never only about the statute. I like to think we have a privacy regime that's composed of a number of components. One is what you're currently engaged with, looking at the statute, but I think we make a huge mistake to focus only on the statute. In many respects, you can have a South African statute, which is one of the best in the world, but in practice it has no lift because there isn't the administrative infrastructure. All the other supporting parts don't exist.

What we need to look at in Canada is the role of Treasury Board. It's the role of access and privacy coordinators and making sure they're appropriately trained, that they're sufficiently senior in an organization, and that they can provide timely advice to lawmakers and government officials. It's about the role, of course, of the Privacy Commissioner.

I come back to talking about flexibility. One of the things that attracts the CBA to the enhanced ombudsman model is that we think it provides a measure of the flexibility we need to meet the evolving world of new and different challenges to privacy.

● (1140)

The Chair: Thank you very much.

We are substantially close to 10 minutes.

We're going to move over to Mr. Tilson.

Mr. David Tilson (Dufferin—Caledon, CPC): Thank you, Mr. Chairman.

My question is to Professor Bennett, who at the the tail end of his presentation made some comments about political parties. I'd like to hear more about that. What are your thoughts as to how they should be regulated? Should it be like everyone else or should it be some other form of regulation?

I've been a member of a political party for some time and I observe other political parties and sometimes they tend to be mischievous. I know people wonder whether that's possible or not, but they are. They're mischievous. Particularly if they're in opposition, they like to tie up the bureaucrats to make them do work that maybe they don't really need. That's only one example, but there might be other examples.

Here's my question. I'm interested in that topic because it seems to me from my observation—some of my colleagues may not agree with me—that they should be regulated, and I'd like to hear more of your thoughts.

Prof. Colin Bennett: Thank you for accepting my invitation.

I wrote a report for the Privacy Commissioner in 2012. At the time Jennifer Stoddart was receiving a number of complaints about political parties. She couldn't do anything about it, so she asked me to do some research on what the main federal political parties were doing in terms of the capture of personal data.

It's complex, but essentially what happens is that the information from the voters list is distributed under the authority of the Elections Act, and then it's supplemented by information from a whole range of an expanding number of sources: telephone polling, door-to-door canvassing, social media, commercial databases, and so on. Techniques that we are currently seeing in the United States have slowly been migrating into Canadian politics. Many people are concerned about this. Political parties are one of the only types of organization in Canada that do not have to abide by the basic common sense, fair information principles, many of which are not controversial. The three main parties do have privacy codes, and they have been making some strides.

What to do is a bit of dilemma, because political parties are *sui generis*. They're not government agencies, so they don't really fit under the Privacy Act. They're not commercial organizations, and therefore PIPEDA would be a stretch.

What I advised both the Privacy Commissioner and the Chief Electoral Officer a couple of years ago when this was discussed was that an interim step would be to negotiate a code of practice. Based on the 10 privacy principles in PIPEDA, the main political parties would be invited to develop privacy codes that would give individuals basic rights of access to their data and would also oblige the large number of workers and volunteers who work for parties during election times to hold that data securely. The adherence to those codes of practice would be a condition for receiving the voters list at the election under the Elections Act.

I thought that was a good interim measure to at least get party officials to get their mind around this issue. It would not, therefore, deal with the complexities of statutory change, which would obviously be controversial.

● (1145)

Mr. David Tilson: Thank you.

Mr. Matt Jeneroux (Edmonton Riverbend, CPC): Thank you all for being here today. Mr. Bennett, thank you as well.

I got scooped a little bit by my colleague here on some of the political party questioning that I had planned to do.

You mentioned that B.C. has legislation. Could you talk a little bit about what that model looks like? Also, is the intent more the protection of the data versus the access to it?

You speak of carrot-and-the-stick argument. It could pertain here as well by saying, “You either do this or you don't get the access to the voters list.” I think the voters list is something that's important, obviously, although I don't know if it's necessarily a political advantage versus being able to engage with people.

Could you speak to that, as well the B.C. question?

Prof. Colin Bennett: Political parties play a crucial role in our democracy in mobilizing voters and in educating the public, and you don't want to have privacy rules in place that hamper that ability.

On the model in B.C., British Columbia is the only jurisdiction in Canada where political parties are covered. That has to do with the particular drafting of our Personal Information Protection Act, which is the substantially similar B.C. legislation that was passed as a result, in the wake of PIPEDA. There have been three investigations, I think, by the former privacy commissioner of British Columbia into political parties. The parties there have been developing codes of practice along the lines that I suggested.

I don't know that this needs to be controversial. We have a principle in this country that you shouldn't be building secret databases. That's the principle behind the Privacy Act. Unless they're exempt for national security reasons, they shouldn't be secret. Individuals should have some right to know what information is being collected on them, how it's processed, and who it's disclosed to.

In most other countries of the world, political parties are covered, with the exception of the United States. There's a gap in Canada. I think the initial step is to engage the major political parties in a process whereby the 10 basic principles in PIPEDA are laid out, then there's a discussion about how those apply to the peculiar context of political campaigning, and then that is translated into some sort of agreeable code of practice for the major political parties. This should not be a race to the bottom.

I've written a great deal on this and I'd be happy to share that with the committee, if you're interested.

Mr. Matt Jeneroux: I know we're over time. I wouldn't mind if we could then in the next round get Mr. Dickson's comments on that aspect.

The Chair: We'll now move to Mr. Blaikie.

Mr. Daniel Blaikie (Elmwood—Transcona, NDP): Thank you very much to everyone for coming and presenting to the committee.

I'm going to direct most of my questions for the time being to Mr. Bennett as well. I apologize to the other panellists for that.

You mentioned that there are some historical systemic reasons that the law in Canada is divided between public and private, and that because of that separation, political parties have been able to fall through the cracks.

What exactly are those reasons? I understood from your presentation that given our situation in Canada, we wouldn't be able to reconcile those two acts and have one piece of governing legislation. What are the reasons? Do you think that is possible? Is it desirable?

● (1150)

Prof. Colin Bennett: Back in the day, the major threat was presumed to be coming from government. It was Big Brother. The history of the Privacy Act was that it followed on from the Access to Information Act and the need to make sure the personal information exemptions in the two statutes were internally consistent.

At that time, it was thought that the private sector could be governed through voluntary self-regulation. For the period of the late 1980s and 1990s, that's what happened. There was a process through the Canadian Standards Association, which I was involved with, that got the major private sector associations to agree to the CSA standard, which then became the basis for PIPEDA.

There are different issues having to do with government agencies and the private sector. With respect to corporations, the role of consent is stronger than it tends to be in government agencies, where the stipulation is that it has to be a statutory requirement, a legislative requirement. Most countries today are starting with a blank slate and think they just have to have one comprehensive statute. Why? It's because it's so difficult to know where the private sector ends and where government begins. That's what technology has produced. The personal information flows backward and forward across those lines in ways that are difficult to regulate.

Having said that, we have to live with those legacies. I don't think there would be any appetite for scrapping PIPEDA, or scrapping the Privacy Act and building a completely new privacy regime.

We live with those legacies. I do think that as far as possible—and this goes to what my colleagues have said—the powers that are included in the Privacy Act for the Privacy Commissioner should be consistent with those under PIPEDA.

Mr. Daniel Blaikie: Recommendation 15 of the Privacy Commissioner is that the act be extended to cover the Prime Minister's Office and ministers' offices. In the absence of that in the current situation, is it the case that private information is largely unregulated in those offices, in the way that it's unregulated for political parties?

Prof. Colin Bennett: Yes, I believe so. It's an issue, because when one of your constituents goes to you with an issue, for example, there's a presumption that the conversation happens in confidence and the information that's being transmitted is not going to find its way into the NDP database, for obvious reasons.

Technology, however, has raised some questions about that under certain circumstances. The ability for members of Parliament, in their capacities as members of Parliament, to capture data that might possibly be of interest when the election comes around is now increased. That, I think, produces a heightened need to do something about this major category of databases that are simply not covered by our privacy regime.

Mr. Daniel Blaikie: If it's the case that personal information isn't regulated in the PMO and it's not regulated within political parties and there are no rules about transfer of government information.... Ordinary MPs don't have access to government databases. Granted, we're approached by our constituents and we have a responsibility—an ethical one, anyway—to respect that information, but the PMO has access to government data, and there are no rules governing its use within the PMO and there are no rules governing the transfer of that information over to political parties, which is then another unregulated environment. Am I understanding that correctly?

Prof. Colin Bennett: You'd have to look at some of the precise exemptions in the Privacy Act. There are certain provisions in section 8 concerning disclosures of government data to members of Parliament in their capacities as members of Parliament, so that is relevant to the question you asked, but there is a gap. I support what the Privacy Commissioner has said in extending the Privacy Act to those offices. It shouldn't be controversial.

● (1155)

Mr. Daniel Blaikie: Am I doing okay for time?

The Chair: You have a minute and a half left.

Mr. Daniel Blaikie: Monsieur Drapeau, if I recall correctly.... Actually, I'm getting confused about who said what now, but I know there's been some advocacy here today for the enhanced ombudsman model. At one time, that was the position of the Privacy Commissioner; since then, he's changed his mind. I'm wondering if those who are advocating that today want to explain why they think the Privacy Commissioner changed his mind and why they think his reasons were not adequate.

Col Michel Drapeau: I obviously don't agree with the reason given by the Privacy Commissioner in his September letter. I think we should go back to the March letter, in which he argued—and I would support it—that it should be a hybrid position. My position is the same as that of the CBA.

Mr. Daniel Blaikie: Okay. What is it, in particular, about the reasons he gives for that change? What do you think happened in his mind that—

Col Michel Drapeau: I don't know. I can't read minds. I presume he had a coffee with the Information Commissioner and they had a meeting of the minds. Really, that would be a plausible explanation as to why.

Frankly, there should be a similarity of approach. I also said before this committee that the Information Commissioner should not have order power. To be consistent, both of them could be using a hybrid model, which seems to be gaining in popularity and efficiency.

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

We now go to the last of our seven-minute questions. Go ahead, Mr. Erskine-Smith.

Mr. Nathaniel Erskine-Smith (Beaches—East York, Lib.): Thanks very much. I want to pick up where Mr. Blaikie left off.

It's interesting that the hybrid model is taking off. We have one jurisdiction that uses it. We have a number of jurisdictions that use the order-making model.

Mr. Dickson, I want to pick up on something you said. I think you said it's more formal and attenuated, would require more procedural fairness, would be less user-friendly, and perhaps staff would have to be divided. B.C., Alberta, Quebec, and Ontario all use this model, and a number of international jurisdictions use this model as well. Is there evidence we can point to that these concerns are warranted?

Mr. Gary Dickson: I think my response would be this. If you take the approach the CBA does—that Canadians have quasi-constitutional rights to have their privacy protected and to have access to government records and government information—then the focus needs to be on accessibility, and accessibility usually translates into a simpler process rather than a more complex one.

When we look at the kinds of complaints that come from different jurisdictions, it's often about delay. It is not so much that decisions of commissioners aren't respected—most times they are complied with, and that's true right across the board, as well as federally—but the issue tends to be one of delay. I think the proposal the Newfoundland committee came up with, which is embedded in the Newfoundland legislation, points a way to an expedited process that can reduce the delay by ensuring a more informal process.

Mr. Nathaniel Erskine-Smith: When we look at B.C., Alberta, Quebec, and Ontario, and then we look at the Newfoundland model, are there differences in formal processes? Do the first four jurisdictions have court-like processes, or is it actually more of an informal process with a commissioner-style model?

Mr. Gary Dickson: There is no question that there is more formality in the process. If you take Alberta or British Columbia, they have people in their office who specifically work on mediation. They have other people in the office whose sole responsibility is writing formal orders in those jurisdictions, so you have that kind of division. It brings in some additional complexity.

Under the existing Privacy Act, there is a provision that the commissioner creates his own procedural rules. There is a provision that nobody is entitled, as a right, to be able to see what the other party has said. They are not entitled to sit in when other people are being interviewed or examined.

I think the Canadian Bar Association's position is that the enhanced ombudsman model provides a significant advantage in terms of flexibility and accessibility.

● (1200)

Mr. Nathaniel Erskine-Smith: I have one more question, and then I would like to get Mr. Bennett's thoughts on the same thing.

With regard to procedural fairness, we have four jurisdictions that have the order-making model, and we have Newfoundland, which has the hybrid model. Would there not be the same procedural fairness concerns?

I can imagine a case in which I bring a complaint to the hybrid model in Newfoundland, and they disagree with me. I want to take that to court, so I have to have been dealt with in a procedurally fair manner by the hybrid model at the first instance. Why is it different when we look at procedural fairness in the hybrid model and in the order-making models?

Mr. Gary Dickson: In Alberta and British Columbia, for example, the process is clearly more formal. There are more opportunities for parties to be able to see what the other side is saying and what other parties are submitting by way of argument. That, of course, is part of procedural fairness.

What happens in an information commissioner's office or a privacy commissioner's office in the ombudsman model is that there is more flexibility. If an issue comes up in the course of an investigation in Alberta or British Columbia, then it is almost like going back to the start. You have to do a bunch of notifications and so on, and start over. There are additional time periods.

With the ombudsman model, if in the course of an investigation another important issue comes up, you provide a more informal notification to the public body. You give them a shorter timeline to provide any additional response. We would see that as being fair, but it is not as rigid a sense of procedural fairness as what you get with an administrative tribunal.

Mr. Nathaniel Erskine-Smith: Thanks very much.

Mr. Bennett, I still have some struggle in understanding why we need a full administrative tribunal with an order-making model. When we look at the four jurisdictions that use the order-making model in Canada, do they have full administrative tribunals? Is that how they operate? Is it incredibly formal? Why would you defend the order-making model?

Prof. Colin Bennett: I think a distinction has to be made between the tribunal model in Quebec and the commission models in B.C. and Alberta. I'm on the external advisory committee for the B.C. information and privacy commissioner, so I may have some biases. I certainly accept Gary's analysis of the pros and cons. There's no issue that it's a complex question.

We should also be very careful about generalizing from the provinces to the federal government and translating models that might work in B.C. or Quebec and think they're going to work in Ottawa.

However, I do favour order-making for a couple of reasons. I think it focuses the mind better. If the B.C. commissioner were here—well, we don't have one at the moment, so the former commissioner—she would say that knowing you have that power focuses the mind of the organization to mediate. Therefore, the kinds of processes that are engaged in mediation should take place more expeditiously, more seriously.

I don't think simply having order-making power necessarily makes it longer. Again, it's apples and oranges, but it's not necessarily.... The other thing about order-making power is it does establish a clarity of law which you do not necessarily get through an ombudsman process.

Mr. Nathaniel Erskine-Smith: There are only a few seconds left.

Mr. Dickson, Newfoundland doesn't have that many complaints. It is a different world when we move to the federal government and the amount of resources that would be brought to bear. Would we not have some concerns about having *de novo* hearings at the court level and losing our efficiency?

Mr. Gary Dickson: I guess the hope is that you're still going to get a relatively small number of matters that end up going to court, and that is the experience right across Canada, and federally too.

The bulk of these matters are dealt with ultimately by recommendations accepted by the public body and implemented by the public body, and that's the bulk of the work, which is why there's so much focus on process. Process and process delays, I think, are probably the number one problem with oversight offices across the country.

Mr. Nathaniel Erskine-Smith: Thanks a lot.

● (1205)

The Chair: Thank you very much.

We will now move to the five-minute round. We are going to start with Mr. Jeneroux.

Mr. Matt Jeneroux: Thank you.

I wouldn't mind going back, Mr. Dickson. We share a similar history, having both been elected to the provincial legislature of Alberta. I don't know if we'd agree on a lot if we had been put back in the same situation, but I wouldn't mind your thoughts, because of your background, on the political party piece that you were speaking with Mr. Bennett on.

Mr. Gary Dickson: My observation would first be that Colin Bennett is very persuasive. I'd say as a result of some of the work he has done, the Canadian Bar Association's access and privacy branches have been engaged with this very issue. Not only did that involve the opportunity to hear Professor Bennett talking about some of the issues, but we've also, as an access and privacy branch, broached that with the Department of Justice and the Office of the Chief Electoral Officer to explore what can be done.

The CBA has no formal position and certainly isn't here to offer a solution, but we're mindful that the former chief electoral officer of Canada has recommended changes to the Elections Act that would require certain standards in terms of protecting personal information collected by political parties. We're mindful that it may be my friend Colin Bennett's persuasiveness, but I noticed that the chief electoral officer in British Columbia has, in an annual report, recommended it's high time that there be some attention paid to developing rules around this issue.

I think the difficulty is determining the best vehicle for doing it. I think there's a growing support and a growing recognition that this area ought not to be left unregulated. This is simply because of some of the huge breaches in the U.S. involving political parties and political organizations that have amassed huge amounts of personal information and then lost it. People are starting to be more concerned about it.

The question is, as Professor Bennett said, what's the ideal vehicle? It clearly wouldn't be, I think, the federal Privacy Act, which is focusing on government institutions. It might be some changes to the Canada Elections Act. It might be developing separate legislation to deal with it. It doesn't nicely fit under PIPEDA, the Personal Information Protection and Electronic Documents Act, either. either. Maybe it would be brand new legislation....

I simply want to say that there is this increasing recognition that there needs to be some means of providing protection for citizens when their personal information is collected, used, and disclosed by political parties.

Mr. Matt Jeneroux: On the topic of changing technology and how we don't know what will come before us and changing the act to keep up with that, Mr. Drapeau, you mentioned that five years is too soon, but 10 years you'd be okay with. We only have a couple of minutes left. Is this better done within policy within the departments, or is it necessary that we put some type of technology requirements within the act?

Col Michel Drapeau: The foundation should pretty well remain stable. I'm saying five years seems to be cautious and too often. I don't know what the formula should be: 10 years, 15 years, and let it work out. I don't see the urgency to do it every five years.

When we're talking about privacy, particularly within the Privacy Act itself, we've got to remind ourselves that privacy is a large mosaic, and the act is only looking at a very finite portion, which is information in records under the control of the federal government. That's it. It doesn't look at any personal, private, confidential information that's passed orally. It doesn't look at information covered by the health care professions, banking, or police forces. I could go on and on. Most of these all have something to do with the protection of, and disclosure of, personal information.

The part that doesn't really work within the federal government at the moment in its administration of the Privacy Act is the disclosure element of it, and what is referred to by the Privacy Commissioner as "consistent use".

I see abuses of that in my own practice. Once the government has this information, there is a tendency to use it and to disclose it for use by federal institutions, consistent with the consent that the person whose personal information has been provided has given to use it for different purposes. That's where problems arise. I see it particularly in some departments that have access to the health care information of individuals. They want to use that, and they do use it, for instance, in the settlement of a workplace grievance. I would question that, and I am questioning it, but at the moment, the Privacy Act allows a department to make that decision—to say they can use this information provided to them about a person's health care for other purposes.

● (1210)

The Chair: Okay. That takes us close to six minutes.

Mr. Dickson, we'll probably get back to you. I do need to move on. Mr. Jeneroux will have an opportunity for more questions.

Mr. Saini is next.

Mr. Raj Saini (Kitchener Centre, Lib.): Thank you very much to all for being here.

I want to pick up on a point that Mr. Dickson raised. He talked about the principles of PIPEDA. The number one principle is accountability. I know, Mr. Bennett, you also mentioned the process of information sharing. My question is a bit broader.

Domestically, we can have written sharing agreements between government institutions and government agencies, which I am sure will be followed by those relevant agencies. My concern is related to a written information agreement with a foreign government.

There are principles involved whereby the foreign government must itemize the requirement for that information and its use or maybe have a necessity test as to why that information is required. My fear is that if you are are divulging information about a Canadian citizen in Canada, and you have the agreement with a foreign government and those principles we have set out in our Privacy Act are met, there is still a lack of guarantee if that information crosses the border and goes to a specific government agency, whether it be national security, defence, or revenue.

How do we maintain the integrity of that information so it will not be divulged to the broader public or divulged within government agencies or institutions of that foreign government? How do we make sure this information is protected once it crosses the border?

Prof. Colin Bennett: You're referring to the U.S. border, I assume?

Mr. Raj Saini: It's any border, really.

Prof. Colin Bennett: That's why I asked the question. For most countries in the world that have comprehensive data protection law, there's an agency similar to the Privacy Commissioner of Canada that the Privacy Commissioner can talk to and have discussions with. If there's any complaint by a Canadian, then there's a process in that other country for that complaint to be investigated.

The problem that we have in Canada is that so much of our information flows over the border to the United States. There isn't an equivalent institution in the U.S. The U.S. has a privacy act that predates our Privacy Act and is from 1974. It's similarly dated. That is administered not through one privacy commissioner, but through a variety of different regulatory agencies.

Your question also relates to the so-called Safe Harbour agreement that was invalidated by the European court. It's now been replaced by a thing called the Privacy Shield, which is mainly for commercial data.

That's all by way of saying that you've asked a very, very good question.

I come back to what I was saying about privacy impact assessments. If they're done properly on both sides of the border, PIAs can go a long way toward ensure that the principles in the Privacy Act are in fact complied with wherever that data goes. There have been some good examples of that. I give the example of the enhanced driver's licence processes, for example. There were PIAs done in Canada and in the relevant institutions in the United States that were reviewed by the Privacy Commissioners in Canada. I don't know whether Gary had something to do with that in his day.

PIAs do play a strong role in alerting the Canadian Privacy Commissioner to any issues that might exist on the other side of the border.

● (1215)

Mr. Gary Dickson: I might just add that if you refer to recommendation 12 of the Privacy Commissioner, you see that he talks about the need to enable him to have discussions with data protection authorities in other jurisdictions. That's frankly all about trying to coordinate enforcement to address the problems with data flowing outside the territorial borders of Canada.

How do you still ensure protection for Canadians? It's partly by having the kinds of agreements you referred to, but it's also by ensuring that data protection authorities can look at joint investigations. The Canadian office has been effective in a number of joint investigations with other national data protection authorities. I think that's a compelling reason that recommendation 12 warrants support.

Mr. Joël Lightbound (Louis-Hébert, Lib.): We're out of time, Mr. Saini.

We'll go to Mr. Jeneroux or Mr. Tilson.

Mr. David Tilson: I would just like to carry on with some of the comments that were raised.

To Mr. Dickson, first I want to compliment you on your brief. The Canadian Bar Association always gives a very thorough brief, and we're always pleased to receive it.

On this issue of information that could go to foreign governments —and we've mentioned the United States in particular—I wonder whether it's possible to enforce unless you have some sort of contract that says, "You can't do this, you can't do this, you can't do this, and if you do it, you're going to get fined or penalized."

You've mentioned it briefly in your brief, Mr. Dickson. Could you perhaps elaborate on what some of your thoughts are on this issue that haven't already been mentioned?

Mr. Gary Dickson: You could do what British Columbia and Nova Scotia have done, which is enact legislation that in fact prohibits certain information sharing outside Canada. They've actually attempted to put restrictions at the front end. It's not always tremendously effective. What you may have is businesses relocating outside your jurisdiction because of some of those limitations in provinces like B.C. and Nova Scotia.

I'd say—I would just be repeating what I suggested earlier—that it's a question of putting in force the strongest and most effective information sharing agreement you can and ensuring that you have a high level of co-operation between international data protection authorities.

I guess the governments need to monitor that information. Privacy commissioners need to monitor those agreements and whether or not they are being complied with in practice.

Mr. David Tilson: Go ahead, Mr. Jeneroux.

Mr. Matt Jeneroux: To go back to the question on the technology piece, Mr. Dickson, you were prepared to comment on how you keep up with technology within the act and whether it's appropriate to put it in the act or somewhere else.

Mr. Gary Dickson: If you look at the Canadian experience, the fact is that this committee is meeting to discuss legislation that was developed in 1983 and has not been substantially changed in over 30 years.

I hear Mr. Drapeau's question about whether five years is too short a time. If you look at Alberta and British Columbia—which for sure have, I think, five of your provisions—they have had requirements for five-year reviews of access and privacy legislation. In both provinces, it has typically resulted in all-party legislative committees looking at it and coming up with a set of recommendations.

The bigger problem in those provinces has been that many of the recommendations aren't acted on. You have the five-year review, some public attention, and a set of recommendations, but the bigger issue is that governments, for one reason or another, often don't implement those kinds of recommendations.

I think five years is appropriate, though, because it not only lines up with a number of Canadian provinces that provide for that statutory review but also ensures that this kind of material doesn't get forgotten. If you rely on a department of justice, or some other department, doing an internal review, it just doesn't attract that kind of attention. When you're dealing with quasi-constitutional laws and rights of all Canadians, the Canadian Bar Association thinks that requires a high level of transparency.

We certainly value the notion of more public reviews done on a regular basis. If there hasn't been a lot of change, then there may be no need for huge amendment. However, it ensures that in a world where technology is changing and so many new risks to privacy keep on developing and appearing, there is an attempt to stay current.

● (1220)

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

Go ahead, Mr. Long, for up to five minutes, please.

Mr. Wayne Long (Saint John—Rothesay, Lib.): Thank you, Mr. Chair, and thank you to all our presenters. They were great presentations, and I think we've had some great questions today.

I was actually going to ask Mr. Bennett some questions about his book, but I think I'm going to ask Mr. Dickson some questions. Also, I think we could all learn as a committee—

A voice: Excellent read.

Mr. Wayne Long: I haven't read it yet, but I will.

I thought our committee could benefit from some of your experiences as privacy commissioner. Were you privacy commissioner in Saskatchewan from 2003 to 2014?

Mr. Gary Dickson: Yes.

Mr. Wayne Long: In one of the articles I read about you, you were described as "a tenacious critic of politicians, bureaucrats and health officials". Would you describe yourself that way?

Mr. Gary Dickson: I'd like to think I was fair, measured, and moderate in all of my recommendations.

Mr. Wayne Long: I guess what I'm getting at is that you were obviously the privacy and information commissioner, and I respect that. You were a member of the legislative assembly. You were also on a committee that oversaw the office of the privacy commissioner.

Can you just elaborate for us on how that experience prepared you for the role? You kind of have a balance of both sides.

Mr. Gary Dickson: I guess the one observation I can share is that there's always a difficulty with access and privacy oversight becoming too complex, too technical, and too formal a process.

When the first parliamentary ombudsman was created in Alberta back in 1967, it was all about providing citizens with a readily available, accessible tool that didn't require a lawyer at your side to trigger an investigation if you thought the government had been unfair or done something improper.

All of my experience drives me to a point where we always have to work harder to ensure that both the systems we put in place and the processes don't become so complex and so time-intensive that we end up not providing the measure of service that Canadians are entitled to and that was envisaged when these laws were initially created and enacted.

It requires work on the part of commissioners, legislators, and people involved in these systems to keep asking themselves if they're being as accessible as they need be, and if they have processes and so on that make this relatively easy for Canadians to use. To the extent we fail to do that, we are failing to meet the purposes of both access to information legislation and privacy legislation.

With that, I'll get off my soapbox.

Mr. Wayne Long: Fair enough, and thanks for that. Obviously, as commissioner you had many achievements and hurdles. Could you give me your single biggest—or maybe your top two—immediate recommendations to reform the Privacy Act?

Mr. Gary Dickson: The first one is our proposal to take the enhanced ombudsman model and run with that. I think there are certainly strengths with the order-making model and I've worked in those jurisdictions that have it, but in terms of providing the highest measure of service to Canadians and the most successful kind of service, I think the enhanced ombudsman model best fits the bill.

Beyond that, the other process is ensuring that the commissioner has a broader range of powers. Parliament has provided the commissioner with diverse powers in PIPEDA, which are appropriate, and we see them being used frequently. The Privacy Commissioner needs a similar arsenal of remedies, tools, and resources when he's dealing with matters under the federal Privacy Act.

● (1225)

Mr. Wayne Long: I know that in 2010 there was an instance of medical records being faxed to the wrong place, and you made a recommendation about that. In 2013, it was still happening. Obviously, you were quite frustrated. You didn't have any non-binding recommendations. Could you elaborate, maybe not just in relation to that case, on the fact that you really didn't have order-making power?

Mr. Gary Dickson: There are some interesting things. If you don't have order-making power, you spend a lot of time thinking about how you can persuade government institutions to do a better job in terms of protecting privacy. I think it puts a premium on creativity, imagination, and some relationship-building, because there's not much sense in writing reports that have all kinds of nice recommendations if there's little prospect they're ever going to be realized.

This ties back into my earlier comment about the need to always ensure that commissioners' offices are being responsive and are accessible to Canadians, and then that they have the appropriate power to be able to ensure remedial action is taken when warranted.

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

We have our last question in the formalized part of the round going to Mr. Blaikie. Then if there are any other MPs who would like to ask some questions, we have some time at the end.

Mr. Blaikie, take us away.

Mr. Daniel Blaikie: Thank you very much.

Professor Bennett, you mentioned that when it comes to PIAs, they can be more effective if they are done earlier in the process.

Is statute the way to try to embed those things earlier in the process? Is it through Treasury Board directives? How do you put those privacy impact assessments at the front end?

Prof. Colin Bennett: The PIAs have been embedded in Treasury Board guidance. My understanding from the Privacy Commissioner is that some departments do a lot of PIAs, while others do very few. They vary in quality a lot.

I did some analysis of PIAs a few years ago, and my conclusion was that they're virtually useless if they're just a statutory checklist to determine if something is legal. They're far more useful when the implications for privacy are considered in a broader context beyond the law and when agency officials are invested in the process of doing that analysis in a recurring way.

The analysis is submitted to the Privacy Commissioner, who gives some feedback, but the understanding is that if there are any subsequent changes to the program, the PIA itself has to be adjusted as a result. That's the kind of early warning system that I think produces an ounce of prevention, and should, in that perfect world, mitigate the chances of data breaches. It should encourage privacy by design. It should encourage the building in of protections at the outset of program development and service delivery, rather than putting them on at the end.

There are plenty of examples in Canada of very good PIAs that fit that model, including some that have been done in the area of border services, but so often they are brief checklists.

Mr. Daniel Blaikie: I guess part of what I'm asking is obviously about the element of organizational culture there. We're reviewing the laws because there's something that should be in the law or changed in the law that would help or facilitate that organizational change, or is it really Treasury Board having to do that hard work of...?

● (1230)

Prof. Colin Bennett: I think there are certain models. Increasingly, privacy impact assessments are included within statutory provisions. They're included, for example, in the new general data protection regulation of the European Union. It's something that all European countries—their organizations there—have to do under most circumstances. It's good organizational practice, but unless it's formalized in law, experience is going to vary and quality is going to vary, and that, I believe, has been the experience of the Privacy Commissioner.

Under Treasury Board guidance, some agencies take that responsibility seriously, others less so. That's why I support his suggestion that you craft some language into the Privacy Act that mandates organizations to do PIAs and consult with the Privacy Commissioner when there are real, substantial risks to privacy.

Mr. Daniel Blaikie: Thank you.

Prof. Colin Bennett: It would formalize what should already be done under TBS guidance.

Mr. Daniel Blaikie: Thank you.

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

Go ahead, Mr. Bratina.

Mr. Bob Bratina (Hamilton East—Stoney Creek, Lib.): One of the most difficult words or concepts in creating legislation is “discretion”.

Monsieur Drapeau, you mentioned recommendation 13, “Provide the Privacy Commissioner with discretion to discontinue or decline”.

Could you remind me of your comments again on that item?

Col Michel Drapeau: In fact, I'm opposing that particular recommendation. The Privacy Commissioner would have the discretion to refuse to investigate a complaint because he would find it frivolous or repetitious or whatever. He would find it, in fact, not to be in accordance with what he would define as a reasonable complaint. I say if you do that, you're talking about a quasi-constitutional right of the individual to use the Privacy Act and to lodge a complaint. It's a human right.

Behind closed doors and in camera, given this discretion, the Privacy Commissioner would deny this individual not only to write a complaint but, if he were to exercise his right to a remedy before a court of law, he couldn't get there. I would oppose that. I'm well aware in some provinces that some of the commissioners have this ability.

Mr. Bob Bratina: There is frivolity and vexation in the world. How would you deal with that?

Col Michel Drapeau: For 33 years, the Privacy Commissioner has had some of these complaints, and no doubt there have been some complaints that might have been frivolous. Some of those presumably won't get the investigative attention, detail, and resources they would otherwise have.

Mr. Bob Bratina: In football, the referee used to have complete discretion. Now we have instant replay and challenge flags, and it seems to be screwing up the game sometimes, so sometimes discretion has been a good thing.

Let me go on to your four-year journey in the complaint that you lodged.

Is there a general way you could speak to our committee on this aspect? You must know so much about this and know where the pitfalls are and why this thing is dragging out. Is there any help you could give us on that one?

Col Michel Drapeau: I think that over the years, the investigative process of privacy has become more and more cumbersome. Maybe more and more the world is designed this way, and we have more procedural fairness. Be that as it may, we now have an investigative process that takes a long time. My suggestion is we don't want to make it any longer than what it actually is, because if you're going to make a complaint, it's a human rights complaint and you want to be sure that you have some form of remedy or some form of resolution as quickly as possible.

Most of the complaints don't go four years, but there are a number of complaints that go to two and three years. Is it an absence of resources? Is it a prioritization of the complaint? I don't know where the problem lies; I really don't, but I'm concerned that it's taking this long. As we speak, there is a 1000- complaint backlog in the privacy office. It will take at least a year before an investigator is assigned to investigate them and come up with some findings and recommendations, so there's a problem even within the existing system. To add order-making powers, as Justice LaForest would have it, is not only expensive but time-consuming, and it's akin to a court proceeding. My comment to you is that the current investigative process at the Privacy Commissioner's office is, in fact, currently longer than most court proceedings.

● (1235)

Mr. Bob Bratina: Resources are an issue. Should we be prioritizing requests? We have international questions and so on, so on the basis that Canadians need service first and given the slow backlog that we've heard about, should some requests be delayed in favour of others?

Col Michel Drapeau: Before we go there, we must make sure that we don't load up the Privacy Commissioner with any task that is not essential to his basic function. His basic function, as it is set out in the Privacy Act, is the investigation of complaints. That's what it is, and that's one of the reasons I basically object to providing him with a function to do public education and research. That could be an open-ended task that will, in fact, draw resources away from his investigative function. His primary role is the investigation of complaints, and that's where the bulk of his assets ought to be.

Mr. Bob Bratina: Mr. Dickson, did you want to comment?

Mr. Gary Dickson: I'd just make this observation. Of course citizen complaints are important, and you have an obligation to do those in a timely way as an oversight office, but if you also have the opportunity to provide input on a new piece of legislation or a new program that may impact hundreds of thousands or millions of Canadians, surely there's high value in that.

Although this office was probably originally conceived as focused almost exclusively on dealing with individual citizen complaints, over time it's evolved so that a substantial and, I think, a critically important part of the mandate is providing advice and commentary to government public bodies when they're developing new technologies, legislation, and programs that may be privacy invasive. I think that's as legitimate as the complaint processing.

Mr. Bob Bratina: Mr. Bennett, would you comment?

Prof. Colin Bennett: The accumulation of complaints, of course, can lead to an understanding about systemic problems, and good commissioners will be able to do that.

I understand what my colleague is saying about the frivolous and vexatious exemption. On the other hand, there are people who do abuse this legislation and put in an extensive number of complaints over and over and over again. We had to deal with this in B.C., and the commissioner there decided to prioritize complaints—to answer your question—by saying that any one person might only have three active complaints going at any one time. That sort of solved the problem.

I do think there should be a public education mandate, a public research mandate. It's already done. It's done under PIPEDA, and if it's done under PIPEDA it's very difficult to distinguish between a private sector issue and a public sector issue these days. The Privacy Commissioner has a very effective contributions program and gives out money for research, which is very valuable in terms of finding out about new technologies and new practices. That is done for public and for private sector issues, so it's very much a question of formalizing what has become the practice of the office over the last 10, 15 years.

Col Michel Drapeau: We may want to look over the past 10 or 20 years, say, at what the percentage has been for investigative resources and whether this number, as a fraction of the overall resources—monetary and personnel—has been diminishing. I think it has been, and as a result, as complaints may increase through time, if we devote fewer investigative resources to attack it, then many complainants will just stand aside and will not file a complaint because they know from the get-go that their complaint will not receive the kind of attention it deserves if they have to wait two years or three years for it to be addressed. That's not a solution, and at the moment I think we are there.

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

Go ahead, Mr. Saini.

Mr. Raj Saini: Thank you.

I have a very broad question.

In your CBA analysis, Mr. Dickson, and from whatever readings I've also done, there has been some talk of reconciling the PIPEDA with some sort of privacy regime to make them more aligned. Of the two starkest differences that have been highlighted in PIPEDA, one is that there is a differential in accountability between a ministerial office and a private enterprise, in that there is a recourse on the government side to have ministerial accountability, while the recourse when you're dealing with private business is that the consumer can go somewhere else and find another service provider.

I also understand that there's the consent issue, because on the private sector side consent is given, but on the public sector side it's more statutory.

In trying to be effective and trying to be efficient, are there any other stark differences that you or Mr. Bennett or anybody else could highlight, or do you think the motivation of the committee should be somehow to reconcile the two so that there are not two different regimes out there, one for the private sector and one for the public sector, so that it would be easier for Canadians to understand one regime and the slight responsibilities that might have to be entertained between the public sector and the private sector?

● (1240)

Mr. Gary Dickson: I'd say, with respect, that the Privacy Commissioner has managed since PIPEDA came into force to be able to address that part of the mandate and deal with concerns with respect to private businesses and private sector organizations, and at the same time to meet the responsibilities under the Privacy Act when it comes to matters related to the public sector.

I'm not sure I feel or understand a need for a higher degree of integration or harmonization than currently exists. I think there are a number of things that are equally important, such as the protection of information, the powers of the commissioner, and so on. Apart from those two issues of accountability and consent, those are divergent matters driven by statute, and I don't see a need to try to reconcile or resolve those into a single approach. They both exist for legitimate reasons that have been tested with the experience of the dual statutes.

Mr. Raj Saini: My main question is this. Outside of those two, are there other stark differences that you see? Could everything else outside of the slight differences that may be apparent between the public sector and private sector have more of a regime that was maybe 80% or 90%—I'm just throwing a number out there—and that could be similar to make it easier for people to understand that these are the slight differences and how to reconcile the two?

Mr. Gary Dickson: From a CBA perspective, those are the two key areas where there are differences for legitimate reasons. I think most of the other elements of PIPEDA work equally well in the Privacy Act. I haven't gone through and itemized each one, but those are the two big differences, which I respectfully submit need to continue to be respected.

Prof. Colin Bennett: I draw your attention to two other things. One is the standard for collection test. The Privacy Commissioner has recommended a necessity for collection related to a government program. I strongly support that. I think that's also relevant in the context of the debates about the revisions of Bill C-51.

The other is that with the basic privacy principles, there's a lot of convergence between the two statutes. There is a big gap in the Privacy Act having to do with security safeguards. The language you find in section 4.7 of schedule I in PIPEDA does not have equivalence in the Privacy Act, and that's a huge gap.

Beyond those, I think all of the other issues have to do with the powers of the commissioner and the tools and the instruments that the commissioner has at his disposal, and that includes mandatory data breaches and PIAs.

Mr. Raj Saini: I have a final question. Both the information act and the Privacy Act were put in place at the same time to be seamless. From what I'm hearing, you feel that both commissioners should have different powers, or should they have the same powers?

Prof. Colin Bennett: Well, I....

Mr. Raj Saini: Let's take one step back.

We finished a report, and the recommendation of the committee was to give the Information Commissioner order-making powers. I think that after that cup of coffee that Mr. Drapeau alluded to, the Privacy Commissioner now also wants the same power.

Is it the case that either we give them the same powers, or there's going to be an imbalance in power?

● (1245)

Prof. Colin Bennett: I think both should have the same powers. I don't know quite how the Privacy Commissioner came to that conclusion. There's been a long series of analysis on this issue.

I would make the point that Canada is probably the only country in the world where the issues of access to information and privacy are seen as two sides of the same coin. In most other places, countries either have a data protection act and no freedom of information, or they have freedom of information and no data protection.

The logic of doing that back in the 1980s was very persuasive. Since then, the two regimes have diverged, particularly as a result of the enactment of PIPEDA, which gives the Privacy Commissioner authority over a range of institutions in the privacy sector and responsibility for a range of issues that were never contemplated when the Privacy Act was promulgated.

The Chair: Well, I think that brings our meeting to a close. I would like to thank our witnesses and my colleagues. Perhaps you'll allow me as the chair to ask the one question in the room that everybody wants to know the answer to but was never brought up: based on last night's debate, is it Trump or Clinton?

I'm kidding, of course.

All kidding aside, Mr. Saini actually asked the question that I had, based on the report that we just issued from this committee, and we're awaiting the government response and legislation. I appreciate the answer, Mr. Bennett. That was the one question I had. If order-making power exists in the information act, then it should probably be counterbalanced with order-making power. Whether we got that right or not remains to be seen.

I think Mr. Drapeau would have something to say about that, but we already know these things.

Thank you very much, ladies and gentlemen, for coming here today. We much appreciate it. I know you'll keep a keen interest in what this committee is doing. If there's any other information that you think we should be aware of throughout our study, please send that to us.

Thank you, colleagues. We'll resume with another meeting on Thursday.

The meeting is adjourned.