HOUSE OF COMMONS
CHAMBRE DES COMMUNES
CANADA

Standing Committee on Access to Information, Privacy and Ethics

ETHI • NUMBER 021 • 1st SESSION • 42nd PARLIAMENT

EVIDENCE

Tuesday, June 14, 2016

Chair

Mr. Blaine Calkins

Standing Committee on Access to Information, Privacy and Ethics

Tuesday, June 14, 2016

● (0855)

[*English*]

The Chair (Mr. Blaine Calkins (Red Deer—Lacombe, CPC)): We're no longer suspended. Thank you very much, colleagues, for getting that little bit of business taken care of.

We're now pleased to get back on track on the study of the Privacy Act. Pursuant to Standing Order 108(3)(h)(i), we are studying the Access to Information Act.

We're happy to have with us this morning the following witnesses: Teresa Scassa, full professor from the University of Ottawa and Canada research chair in information law; David Lyon, who is joining us by video conference, professor at Queen's University; and Lisa Austin, associate professor, University of Toronto, faculty of law, in the David Asper Centre for Constitutional Rights.

Thank you very much for taking the time to join us, and thank you for your patience as we dealt with a little bit of business at the start of our committee meeting. We just finished up our review of the access to information legislation, and now we're going to continue on with our review of the privacy legislation.

We're going to ask each of you to do about a 10-minute presentation. Then we'll proceed to rounds of questions and hopefully use up the full two hours.

Based on the order that they appear on my sheet, we'll begin with Teresa, please.

Ms. Teresa Scassa (Full Professor, University of Ottawa, Canada Research Chair in Information Law, As an Individual): Thank you, Mr. Chair, and thank you for the opportunity to address this committee on the issue of the reform of the Privacy Act.

I have had a chance to review the commissioner's recommendations for Privacy Act reform and I am generally supportive of these proposals. I'm going to be focusing my remarks today on a few specific issues that are united by the theme of transparency.

Greater transparency with respect to how personal information is collected, used, and disclosed by government enhances privacy by exposing practices to comment and review and by enabling appropriate oversight and accountability. At the same time, transparency is essential to maintaining public confidence in how government handles personal information.

The call for transparency must be situated within our rapidly changing information environment. Not only does technology now enable an unprecedented level of data collection and storage, but enhanced analytic capacity has also significantly altered the value of information in both public and private sectors. This increased value provides temptations to overcollect personal information, to share it, to mine it, or to compile it across departments and sectors for analysis and to retain it beyond the period required for the original purposes of collection.

In this regard, I would emphasize the importance of the recommendation of the commissioner to amend the Privacy Act to make explicit a “necessity” requirement for the collection of personal information, along with a clear definition of what “necessary” means.

The goal of this recommendation is to curtail the practice of overcollection of personal information. Overcollection runs counter to the expectations of the public, who provide information to government for specific and limited purposes. It also exposes Canadians to enhanced risks of negligence, misconduct, or cyberattack, which can result in data breaches.

Data minimization is an important principle that is supported by data protection authorities around the world and reflected in privacy legislation. The principle should be explicit and up front in a reformed Privacy Act.

Data minimization also has a role to play in enhancing transparency. Not only do clear limits on the collection of personal information serve transparency goals, but overcollection also encourages the repurposing of information, improper use, and over-sharing.

The requirement to limit collection of information to specific and necessary purposes is tied to the further requirement on government to collect personal information directly from the individual, where possible. This obviously increases transparency, as it makes individuals directly aware of the collection.

However, there are many exceptions to this general rule. These exceptions include circumstances in which information is disclosed to an investigative body at their request in relation to an investigation or the enforcement of any law, or when it's disclosed to government actors under court order or subpoena. Although such exceptions may be necessary, they need to be considered in the evolving data context in which we find ourselves.

Private sector companies now collect vast stores of personal information, and this information often includes very detailed core biographical information. It should be a matter of great concern, therefore, that the permissive exceptions in both PIPEDA and the Criminal Code enable the flow of massive amounts of personal information from the private sector to government without the knowledge or consent of the individual.

Such requests or orders are often, although not always, made in the course of criminal or national security investigations. The collection is not transparent to the individuals affected, and the practices as a whole are largely not transparent to the broader public and to the office of the Privacy Commissioner.

We've heard the most about this issue in relation to telecommunications companies that are regularly asked or ordered to provide detailed information to police and other government agents. It should be noted, however, that many other companies collect personal information about individuals that is highly revelatory about their activities and choices. It is important not to dismiss this issue as less significant because of the potentially anti-social behaviour of the targeted individuals. Court orders and requests for information can and do encompass the personal information of a large number of Canadians who are not suspected of anything. The problem of tower dump warrants, for example, was recently highlighted in a case before the Ontario Supreme Court. The original warrant in that case sought highly detailed personal information on about 43,000 individuals, the vast majority of whom had done nothing other than use their cellphones in a certain area at a particular time.

Keep in mind that the capacity to run sophisticated analytics will increase the attractiveness of obtaining large volumes of data from the private sector in order to search for an individual linked to a particular pattern of activity.

Without adequate transparency regarding the collection of personal information from the private sector, there is no way for the public to be satisfied that such powers are not abused. Recent efforts to improve transparency—for example, ISED's voluntary transparency reporting guidelines—have focused on private sector transparency. In other words, there has been an attempt to provide a framework for the voluntary reporting by telecommunications companies of the number of requests they receive from government authorities, the number they comply with, and so on. However, not only are these guidelines entirely voluntary, but they are limited to the telecommunications sector, whereas disclosures may be sought from any private sector company.

● (0900)

They also only address transparency reporting by the companies themselves. There are no legislated obligations on government actors to report in a meaningful way, whether publicly or to the Office of the Privacy Commissioner of Canada, on their harvesting of personal information from private sector companies. I note that the recent attempt by the OPC to audit the RCMP's use of warrantless requests for subscriber data came to an end when it became clear that the RCMP did not keep specific records of these practices.

In my view, a modernization of the Privacy Act should directly address this enhanced capacity of government institutions to access the vast stores of personal information in the hands of the private sector. The same legislation that permits the collection of personal information from private sector companies should include transparency reporting requirements when such collection takes place. In addition, legislative guidance should be provided on how government actors who obtain personal information from the private sector, either by request or under court order, should deal with this information. Specifically, limits on the use and retention of this data should be imposed.

It's true that the Criminal Code and PIPEDA enable police forces and investigative bodies under both federal and provincial jurisdiction to obtain personal information from the private sector under the same terms and conditions, and that reform of the Privacy Act in this respect will not address transparency and accountability of provincial actors. This suggests that issues of transparency and accountability of this kind might also be fruitfully addressed in the Criminal Code and in PIPEDA—the reform of which this committee is also considering—but this is no reason not to address it in the Privacy Act. To the extent that government institutions are engaged in the indirect collection of personal information, the Privacy Act should provide for transparency and accountability with respect to such activities.

Another transparency issue raised by the commissioner relates to information sharing within government. Technological changes have made it easier for government agencies and departments to share personal information, and they do so on what the commissioner describes as a massive scale.

The Privacy Act enables personal information sharing within and between governments, domestically and internationally—in specific circumstances for investigations in law enforcement, for example, or for purposes consistent with those for which it was collected. Commissioner Therrien seeks amendments that would require information sharing within and between governments to take place according to written agreements in a prescribed form. Not only would this ensure that information sharing is compliant with the legislation, but it would also offer a measure of transparency to a public that has a right to know whether, and in what circumstances, information they provide to one agency or department will be shared with another, or whether and under what conditions their personal information may be shared with provincial or foreign governments.

Another important transparency issue is mandatory data breach reporting.

Treasury Board Secretariat currently requires that departments inform the OPC of data security breaches, but the commissioner has noted that not all comply. As a result, he is asking that the legislation be amended to include a mandatory breach notification requirement. Parliament has recently amended PIPEDA to include such a requirement. Once these provisions take effect, the private sector will be held to a higher standard than the public sector unless the Privacy Act is also amended.

Any amendments to the federal Privacy Act to address data security breach reporting would have to take into account the need for the commissioner and for affected individuals to be notified when there has been a breach that meets a certain threshold for potential harm, as will be the case under PIPEDA.

The PIPEDA amendments will also require organizations to keep records of all breaches of security safeguards, regardless of whether they meet the harm threshold that triggers a formal reporting requirement. Parliament should impose a requirement on those bodies governed by the Privacy Act to keep and to submit records of this kind to the OPC. Such records would be helpful in identifying patterns or trends within a single department or institution, or across departments or institutions. The ability to identify issues proactively and to address them either where they arise or across the federal government can only enhance data security, something which is becoming even more urgent in a time of growing cybersecurity threats.

I'm going to stop my comments there.

Thank you very much, Mr. Chair.

● (0905)

The Chair: Thank you very much.

I think we're going to have a very interesting conversation with you.

We'll now go to Mr. Lyon, please, for up to 10 minutes.

Mr. David Lyon (Professor, Queen's University, As an Individual): Thank you very much for inviting me to participate in what I think is an important initiative. The Privacy Act is out of date, and Canadians urgently need a new and strong law that speaks to the tremendous technological changes and political economic shifts that have occurred since the 1980s.

In general, I am in agreement with and grateful for the proposals made by the Privacy Commissioner. At the same time, I should make it clear that I am not a lawyer, and nor do I have any legal expertise. I speak as a university professor who has been engaged in the social sciences. I direct the Surveillance Studies Centre at Queen's University.

My last book was *Surveillance after Snowden*. The large-scale team project I direct at the moment is called Big Data Surveillance. The book that I'm currently working on is *The Culture of Surveillance*. I mention these simply to give you some sense of the angle from which I am coming and from which I speak, which is the broad context of this act rather than the details.

Let me start by pointing out that there's a publication our research team brought out a couple of years ago. It's called *Transparent Lives: Surveillance in Canada*. It's a highly accessible study of the trends in surveillance today. I commend it to the committee. You can get it from any good bookstore, or it is downloadable online.

[*Translation*]

It is also available in French, under the title *Vivre à nu: La surveillance au Canada*.

[*English*]

This book encapsulates the key issues about surveillance in the 21st century and gives a comprehensive background, for anyone who would like to see it, for the need for a changed privacy law.

The trends that it examines, and for which it offers Canadian examples, include the rapid pace of increasing surveillance, the role of security concerns in prompting surveillance, the blurring of public and private sectors—Snowden's disclosures make this very clear—the ambiguity of personal information, the growth of mobile and location-based surveillance, the embedding of surveillance in everyday environments—sometimes discussed as the Internet of Things—the growth of biometrics, and social surveillance on Facebook, Twitter, and other media.

The Privacy Act is premised on some rather fixed ideas about personal information in terms of who collects it and where, if at all, it travels. Today, fluidity rather than fixity is the order of the day. Words such as “databases” define the old document, and this suggests silos in contrast to the multiple conduits through which data flow today. Information was seen then as pertaining to those specific sites, and sharing information could only happen under certain circumstances.

There still, of course, need to be limits on this practice, as we've just heard, and it has to be acknowledged at the same time that information sharing today exists on a scale that wasn't dreamed of in the 1980s, a scale that would be very difficult to quantify, let alone control.

It also occurs across boundaries assumed by the distinction between government activities and commercial ones in the two main federal laws of 1982 and 2004. The easy traffic in each direction between these domains was never envisioned in the 1982 act, and this is a key issue to be confronted in any review.

At the same time, surveillance can and does happen without there being any obvious handles for identifying personal information. The very category of personal information is badly blurred today. Once you could have imagined that this category would cover such matters as name, address, telephone, and perhaps some official identifier such as the social insurance number. Today, license plates captured by highway cameras count, and although this is controversial, so do IP addresses on computers.

Moreover, one can be identified through facial recognition. The software, for example, that is routinely used by Facebook doesn't even require a Facebook account in order for it to function. Indeed, it's relatively straightforward to identify people with no obvious identifying information provided. A Montreal study recently showed that 98% could be positively identified with birthdate, gender, and postal code without names and addresses being known.

● (0910)

The post-Snowden debate over whether or not metadata around phone and Internet messages count as personal data is another example. This is supposedly contextual, sometimes dismissed misleadingly as phone book-like information rather than content, but metadata is frequently more revealing, not less.

The two items mentioned refer to socio-technical and political-economic changes that have occurred over the past 40 years, and I wish to turn to matters of research and education, on which the commissioner also speaks.

On the one hand, much more research is required to properly understand the momentous changes that have occurred since the 1980s. It must be stressed that these are both socio-technical and political-economic changes and cannot safely be reduced to technical and legal categories.

For a number of years the commissioner has overseen a very successful program of funded research under the contribution scheme, but given the magnitude of the issues and their centrality to matters from national security to domestic life, much more is needed if the law governing the uses of personal data is to be kept up to date in a way that genuinely addresses all whose lives are touched by surveillance of all kinds, which is everyone.

This research program could be expanded under the act as a background to the revision of the Privacy Act, but it could also be widened by requests for surveillance and privacy research by the Tri-Council or by the Royal Society of Canada for a dedicated report on surveillance and privacy law in Canada. I suggest that such study is needed before the law can be revised.

On the education front, it is clear that much has to be done here, and this too could be coordinated by the Privacy Commissioner with an expanded brief.

In the 1980s, computing still meant primarily what were called “mainframes”, and the era of personal computing—not to mention the popular diffusion of distributed systems, mobile devices, and the cloud—was yet to flower. In that decade, if you wished to connect with others, for example, or with what would emerge in the 1990s as the Internet, you had to use a cumbersome system of plugging your land-line phone handset into rubber sockets—I don't know if anybody remembers that; it was called an acoustic coupler—to create a very uncertain data link modem.

Today computer devices and networks have proliferated in ways that demand fresh approaches to what I think should be called “digital citizenship suitable for all ages”. All Canadians need to know their rights, understand the issues, and engage actively and in an informed way. This is not a minority option. This is not something on the side. This again could be initiated by the commissioner. It could accompany the new law and could refer to the work of many other agencies where such matters are central, and in my little brief I've put some references for you.

While I believe all the above are essential components of a revised privacy law, it seems to me that the nature of the debate also has to shift to consider carefully the underlying ethical direction that should be encouraged to enable the most just and fairest uses of digital media and personal information and to exploit the best purposes of the great potential of digital technologies.

The very notion of privacy, of course, has undergone considerable change since the 1980s. These are not minor or peripheral matters and cannot be addressed in merely technical or legal ways. It's not only that privacy in some narrow sense might be violated by the misuse of these powerful technologies, but rather that our opportunities to live as free and fulfilled human beings are enhanced or curtailed by surveillance, whether by government or corporation.

As Eric Stoddart argues, much monitoring and tracking today is the surveillance of others. We would do well to consider how surveillance could be harnessed for human flourishing, which would be surveillance for others.

● (0915)

Thank you very much.

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

We now go to our last witness.

Ms. Austin, you have up to 10 minutes, please.

Ms. Lisa Austin (Associate Professor, University of Toronto, Faculty of Law, David Asper Centre for Constitutional Rights, As an Individual): Thank you.

I thank you for inviting me to appear before you today. I appreciate the opportunity. I have prepared a written submission for your committee. It's currently being translated and will be distributed to you. My comments will be a summary of that submission. I welcome your further questions.

The basic point I want to stress to you today is that Privacy Act reform must take account of the Canadian Charter of Rights and Freedoms and its protections for privacy. We should not think that compliance with the Privacy Act means compliance with the charter, and we should not think that strengthening the Privacy Act's adherence to fair information principles means that it's thereby consistent with the charter's protection for privacy.

It's crucial that we understand this, for we're now in an era when the government collects large amounts of information about individuals and shares this both within government and with other governments, including foreign governments. This is not just for the provision of social services but for law enforcement and national security purposes, as both the prior witnesses stressed as well. Indeed, when the former government introduced Bill C-51 and the new Security of Canada Information Sharing Act, Canadians were told that because the Privacy Act applied and the Privacy Commissioner would provide review, there would be an appropriate balance between protecting the privacy of citizens and ensuring national security. This is an illusion, and it's a dangerous one.

The Privacy Act is quasi-constitutional legislation, that's true. The Supreme Court has said that multiple times. However, it should not be equated with the constitutional protection of privacy rights. The Privacy Act is based on what have come to be known internationally as "fair information principles". Its basic model is a response to the growth of the administrative state and its accompanying information practices. An individual seeking government services in a social welfare state context has an interest in receiving those services. The administration of those services requires personal information to be collected and processed, so the individual interest in relation to this personal information is not about preventing its collection, use, or disclosure, but in preventing the overcollection of personal information or its subsequent uses or disclosures for different purposes, as well as in ensuring that the information is accurate. The central individual entitlement is to have access to the information the state holds about oneself, and to correct it for inaccuracies. This law was never really meant to apply to the context of law enforcement and national security in any robust way, and many of its exceptions capture those uses.

In contrast, the constitutional protection of privacy in Canada has developed largely in relation to section 8 of the charter, although privacy has also been protected through section 7. Its central paradigm is its search and seizure context, where the state seeks information in relation to law enforcement investigations. Here the individual interest lies completely in opposition to the state interest. It is a coercive relationship. The central individual entitlement is to have state access protected through the warrant requirement and the reasonable and probable grounds standard. These are two different frameworks, but they need to be integrated if we think the Privacy Act has anything to say to the increasing information practices the government employs in the context of law enforcement and national security. Charter review should be built into a strengthened Privacy Act review, particularly in this context.

In light of this, I have four recommendation I want to offer to you. Again, those are outlined in the written submission.

First is an interpretive principle. We recommend that the Privacy Act should include a reference to privacy rights protected by the Canadian Charter of Rights and Freedoms. Put a reference to it in the purpose section to allow for arguments to be made in reference to the Charter of Rights and Freedoms.

Our second recommendation is that government information practices should be reviewed for compliance with charter rights. The necessity standard that the Office of the Privacy Commissioner of Canada is advocating is not adequate. It's better than what we have, and it's good in many contexts, but it's not adequate.

Why do I say that? Charter rights can be at issue with the collection, use, or disclosure of personal information. The charter is engaged when there's a reasonable expectation of privacy; it's not simply when personal information is collected, used, or disclosed, but where there's a reasonable expectation of privacy. The Supreme Court of Canada has repeatedly held that information that has been collected by the state for one purpose can retain a residual reasonable expectation of privacy in relation to other purposes, including disclosure to foreign states.

● (0920)

Engaging in something like a necessity test modelled after the Oakes test for section 1, which is what the Privacy Commissioner advocates, is not going to be adequate in this context. Why? The section 8 reasonable and probable grounds test, which is the basic standard, is not a test that says the state gets access to information if it is necessary for a law enforcement purpose; it's a test that says that "...law enforcement goals hold sway only at the point marked by the probable effectiveness of reaching that goal." This idea of probable effectiveness is not part of the the section 1 jurisprudence to date.

It's actually quite unclear when a breach of either section 7 or section 8 of the charter can be upheld under section 1 of the charter. That's because there's an internal balancing in section 1 as well as as one in section 7, and courts are loath to uphold them under section 1, so we should not be quick to regularize some kind of section 1 analysis until we actually import the charter privacy protections, particularly in the context of state use of this information for law enforcement and national security purposes.

Therefore, we recommend that the use or disclosure of personal information for law enforcement investigative or national security purposes should be subject to a review that reflects the protection of an individual's charter rights under sections 7 and 8, and not simply be reviewed on a necessity standard.

Our third recommendation is that the Office of the Privacy Commissioner be empowered to undertake charter review of government information practices. Charter review of these information practices should not be a burden placed on ordinary Canadians to both discover information practices that are difficult for them to see and understand—to come to know what those practices are—and to challenge them in court. It should not be a burden on the individuals to initially challenge these things in court in a context where we have an access to justice crisis in this country. Instead, we should build it into the Office of the Privacy Commissioner's function.

However, it's also important that this be reviewed on a standard of correctness in the courts. It should not be built into an administrative process such that the courts are then reviewing charter complaints on a reasonableness standard. It should be correctness.

Therefore, we recommend that the exemptions, particularly those under sections 7 and 8 of the Privacy Act for uses and disclosures of personal information without consent, should be subject to charter review conducted by the Privacy Commissioner, subject to judicial review on a standard of correctness.

Our fourth recommendation is that you strengthen the obligation of accuracy under the Privacy Act.

Inaccurate information can have grave consequences on fundamental rights and freedoms. This is one of the tragic lessons from the Arar commission. Currently the obligation of accuracy is in subsection 6(2) of the act. It applies to uses of personal information, but it should apply to uses and disclosures of information, not just uses. It's currently confined to administrative purposes, and it should be broadened to all the purposes that it's used for.

I think that the act should also be modernized to recognize what academics are increasingly terming "algorithmic responsibility"—that is, the idea that the issue is not just the accuracy of the information that's collected, used, or disclosed, but the accuracy of information processing methods used by the government.

In an era of big data, an era when vast amounts of information are being collected and analyzed in different ways, we need to be concerned about the accuracy of those methods of analysis. We need to be concerned that they're not building in biases, for example, or other forms of inaccuracy. Therefore, we recommend that subsection 6(2) of the act be amended to impose an obligation to ensure the accuracy of any personal information that is used or disclosed by the institution for all purposes. The obligation of accuracy should also apply to methods of information processing.

I'll end my comments there.

Thank you.

● (0925)

The Chair: We're going to have a great conversation.

Thank you, Ms. Austin.

We're going to start with a seven-minute round. We have four questioners for seven minutes each. Our first questioner is Mr. Erskine-Smith.

Mr. Nathaniel Erskine-Smith (Beaches—East York, Lib.): Thanks very much to all three of you.

Ms. Austin, I want to start with a couple of your recommendations with respect to including explicit reference to the charter, and then explicitly stating that it would be reviewed on the standard of correctness.

My understanding is that the charter applies anyway, and that all charter analysis is on the standard of correctness as it is. You're effectively saying to codify that in the Privacy Act itself. The substantive change, I understood from your submission, would be that the Privacy Commissioner would be tasked with reviewing information sharing and information use for charter compliance. Everything else is a codification, rather than a change of the law.

Ms. Lisa Austin: The trend in jurisprudence is that when you have an administrative decision-maker, such as the Office of the Privacy Commissioner, the courts are highly deferential, including sometimes with respect to charter issues. It's something that the David Asper Centre has been tracking and is concerned about. They're concerned that on charter issues, the courts actually have the last say on a standard of correctness. That's worth putting in.

The rest is, yes, to build in the charter review initially, because you can have Privacy Act compliance that still raises charter issues. You can have information sharing that is perfectly compliant with the Privacy Act as it now stands, or even compliant with the Privacy Act if you amend it according to the Privacy Commissioner's recommendations, but would still raise charter issues.

That charter review shouldn't be bolted on after the fact and the burden of it be placed on citizens. It should be built in from the start.

Mr. Nathaniel Erskine-Smith: My next question is for all three.

Ms. Austin, you made reference to the Security of Canada Information Sharing Act, which now permits 17 government institutions to disclose information among one another, and this can be extended by cabinet to other individuals and organizations and departments. As we look to changing the Privacy Act to require, for example, written agreements for information sharing, would that get at the problem under the Security of Canada Information Sharing Act? If not, what other substantive changes should we make to the Privacy Act in particular that would get at Canadians' concerns about overly broad information sharing under what was BillC-51?

Ms. Lisa Austin: I would say that the written agreements are a start. Again, I would want charter compliance built into them, because some of this information sharing can raise charter issues, and these need to be flagged early on.

The charter jurisprudence is clear in saying that just because one government institution has information that it has collected for one purpose doesn't mean it can use it for subsequent purposes; sometimes a charter issue is flagged, and there needs to be charter compliance. That can also happen with sharing it with foreign states.

Section 8 was triggered in the Wakeling decision, although there was a disagreement on whether the provisions in the Criminal Code were reasonable. In the end, they were found to be reasonable.

The written agreements are a start, then, but you need the charter review of the information sharing, because some of it will raise charter issues, but not all of it, hopefully. You thus need to build it in at the beginning.

I would also say that whenever some of this information is shared, particularly with foreign governments, the accuracy issue is enormous, so building in an obligation of accuracy is important.

I don't see how the current obligation of accuracy actually applies, because it's about use for administrative purposes. If you're sharing this information for national security purposes or for transnational law enforcement purposes, it seems to me it's not part of that, but it's crucial that accuracy be built in. You could, through regulations, specify perhaps what that might mean in particular circumstances, but I think it's an absolutely crucial amendment.

Mr. Nathaniel Erskine-Smith: Are there any comments from the other two witnesses?

Ms. Teresa Scassa: With respect to the written agreements—and I think the commissioner refers to written agreements in a prescribed form—that the devil's going to be in the details. It will depend to a very large extent on what that prescribed form is, how detailed those written agreements are, and what the exceptions are. I think there's always a risk, particularly in the law enforcement and national security arena, of creating broad exceptions or limitations on what is disclosed.

Obviously the tension is the balance between privacy and security in that context, but the effectiveness of any written agreements, I think, really will depend on what is required to be in those written agreements, how transparent they will actually be, and to what extent exemptions from those requirements would blunt their effectiveness.

● (0930)

Mr. Nathaniel Erskine-Smith: Do you foresee written agreements in a schedule to the act, for example, following a precedent, or would these be written agreements that would be different on an individual basis between departments, depending upon the departments and depending upon the type of information they're sharing?

The Chair: Mr. Lyon, do you have something you want to add to that? I know that Mr. Erskine-Smith opened the floor up to everybody, but it looks as though you wanted to jump in. I want to make sure I give you a choice or a chance.

Mr. David Lyon: The only thing I wanted to say was that I couldn't hear very clearly what the question was. The mike didn't seem to be picking up the questioner.

Mr. Nathaniel Erskine-Smith: My question was with respect to whether one would envision a precedent being set out in a schedule to the act or whether we're looking at different kinds of agreements between departments. Would we have one standard form that could be departed from if the departments wished to do so, one standard form that they could rely upon?

Mr. David Lyon: Okay. Yes, I think the comments of Lisa Austin spoke directly to that and I think that's the way that I would answer.

Ms. Lisa Austin: The one point of the written agreement that I'm not sure about or that I would put as a question to you to think about is that when information-sharing practices are set up, it seems to me that it's not just about having an agreement in place that you write up: you're going to have some technical tools for dealing with the data, especially if you're dealing with large amounts of data that you're sharing in different ways, so what's the oversight for the technical system that you're setting up?

The written agreement seems like an advance over what the situation is now. I agree with the Office of the Privacy Commissioner's submissions on that point, but isn't there also oversight of the technical infrastructure that we're creating? How do you make sure that it is reviewed properly as well, and in a transparent manner? That is something to think about.

Mr. Nathaniel Erskine-Smith: I think I'm out of time.

Ms. Scassa, you mentioned that you are largely in agreement with the Privacy Commissioner's recommendations.

Where any of you disagree with the recommendations, could you please advise the committee today or later in writing? It would be appreciated.

The Chair: I'm sure we'll get to any discrepancies.

Thank you very much, Mr. Erskine-Smith.

Mr. Kelly, you have up to seven minutes.

Mr. Pat Kelly (Calgary Rocky Ridge, CPC): Thank you.

Thank you all for attending our meeting. This is great information.

I'll start with Mr. Lyon. I haven't had the benefit of reading your book. Could you talk about, maybe even on an anecdotal basis, the different specifics of how the surveillance culture, as you've described it, works itself out at ground level? What are the specific concerns or specific activities that contribute to this culture, and how do these intersect with the Privacy Act?

Mr. David Lyon: It's a great question. I haven't finished writing the book yet, but what we're working on is looking at the ways in which.... Well, it's in contrast with the situation in the 1980s, when these kinds of issues were still seen as relatively discrete in that they didn't apply to everyone. In what I'm calling a surveillance culture, people have a kind of surveillance imaginary, a sense of what's going on, and engage in practices that relate to surveillance, whether it's avoiding certain kinds of surveillance or actively participating in them or complying or negotiating or whatever.

In talking about surveillance culture, I'm trying to draw attention to the fact that there's no point in talking about a surveillance state anymore, or even a surveillance society, although those are important concepts. We have to think about the ways in which people in everyday life interact in numerous ways, and increasingly, with all kinds of surveillance.

Of course, I'm understanding surveillance in the broad sense of any kind of activity or experience of gathering and analyzing personal information for all kinds of purposes, whether they be for influence, control, management, or whatever. I'm working with a fairly wide definition of surveillance that, again, was not envisaged by those who were writing the Privacy Act in the 1980s. I'm thinking of situations, for example, where people are engaged with social media and are actually very aware of the kinds of risks that they take in certain kinds of communication, certain kinds of web-browsing, and so on and so forth.

That culture of surveillance that is developing in many different aspects actually has an effect on the ways in which surveillance is carried out and privacy is maintained, and for all that some say that privacy is less of a matter of interest to younger people who are using social media, in fact you discover that there's a very sophisticated and complex understanding of privacy. This relates both to the big issues of the charter, for example, and to the small issues, such as which particular party you do or do not want your own communications to be open to.

Therefore, I'm thinking of something that is developing in Canada and in other countries that affects our understanding of what it is to be enjoying privacy, our understanding of what it is to be under surveillance, and how those understandings and those practices make a difference to the ways in which surveillance actually works—to its very efficacy—and also to privacy.

● (0935)

Mr. Pat Kelly: Thank you for the answer. I appreciate it very much. I'm just going to try to squeeze in a couple of questions to other witnesses before my time runs out.

Ms. Austin, just to help me understand our subject matter here, could you give me an example of a specific activity that is compliant with the act but not charter compliant? You spoke of the disconnection between the charter and the act. Could you give some specific activities?

Ms. Lisa Austin: Under the act, for law enforcement purposes it's permissible to disclose personal information without consent upon the request of an agency that's listed in the regulations. If there's a reasonable expectation of privacy in that information, you need a warrant for that. Under the Privacy Act, if you're requested and you hand it over, that's fine, but under the charter, you might need a warrant. You can be Privacy Act-compliant but have a problem with the charter.

It's the same with foreign governments. Under the Privacy Act, information can be shared with foreign governments through an arrangement—it doesn't even have to be written—and there is no Privacy Act issue, but there could be a charter issue. Wakeling v. United States of America is a Supreme Court of Canada decision that suggests that section 8 of the charter is engaged when information is shared with a foreign state. That was information that was actually lawfully collected through a Canadian wiretap in that case.

You can have information that the government has and shares with a foreign state. The Privacy Act says that's perfectly okay if it's pursuant to an arrangement and it's for law enforcement purposes, but the charter might say to wait a minute and that you need a heightened set of protections in those particular circumstances. It might be a warrant or it might not be a warrant; it might be subsequent protections on the uses of that information. “Safeguards” is the language that the Supreme Court of Canada tends to use, but it's not currently in the act.

Mr. Pat Kelly: Ms. Scassa, you spoke about third party collection of data, by which I am assuming your are referring to information collected for commercial reasons by a private business or information transferred between private individuals that through a second transfer ends up with an agency of government.

Could you give me some examples of how government ends up with information collected by a third party?

● (0940)

Ms. Teresa Scassa: Yes, that's essentially through information-sharing provisions that are found in both the Criminal Code and in PIPEDA, the private sector data protection legislation, which allows for disclosure. In the Criminal Code, it's disclosure in the context of law enforcement; in PIPEDA, it can be law enforcement, but it can be in relation to an investigation or in relation to the enforcement of any law of Canada or a province, so the range of regulatory purposes is much broader.

That information can be requested from the private sector company and can be provided on request if the private sector company is wiling to disclose that information, or it can be sought through a court order. In either event, the information will be collected by government. That collection is not directly from the individual but from the private sector company. It can be information that is very specific to an individual, but it can also be—and this has been the case now with some court orders—bulk information that is going to be searched or analyzed for patterns.

The Chair: Thank you very much, Mr. Kelly. We've gone a little bit past.

Mr. Dubé, you have up to seven minutes, please.

[*Translation*]

Mr. Matthew Dubé (Beloeil—Chambly, NDP): Thank you, Mr. Chair.

My thanks to the witnesses for joining us today.

Ms. Austin, I think it was you who talked about the importance of government agencies gathering data in order to develop social programs. However, the problem is not just about gathering data; it is also about storing the gathered data, if I may put it that way. Think of recent examples, specifically the Canada Revenue Agency; whether personal information was lost or accidentally disclosed doesn’t really matter.

What should be done to make sure that data are not only collected appropriately but also protected appropriately once they have been gathered?

The same question goes to the other witnesses too.

[*English*]

Ms. Lisa Austin: I think one of the important issues around how we store and protect information is that it also has charter dimensions to it.

The recent jurisprudence in the Supreme Court of Canada has been very strong on the idea that you need safeguards around information. For example, when there's an analysis of the reasonableness of a law in the context of a charter privacy issue, there's an increasing discussion on the question of safeguards, in that if you don't safeguard the information properly, that can be the charter breach.

The gravity of that issue is that it's not some sort of technical, administrative element to the Privacy Act. There are serious charter issues in not safeguarding that information properly that the courts are starting to really pay attention to.

My own view is that we haven't built in enough on the technical side of the review process. We still seem to be thinking about it much along the lines of what David Lyon has been talking about, seeing personal information as if it's discrete information collected in a kind of paper environment that's shared in filing cabinets, but these are information systems. They're technical systems. It's software. It's algorithms. The whole issue of safeguarding has an incredible technical side to it as well. Getting the legal standards right, whether it's in the legislation or in regulations, is important, and getting the oversight right is important, but there's a whole technical side to that too. I think we're not building enough technical expertise into the review process.

As to what that looks like particularly, I don't have an answer for you, but I think we need to really understand the fluidity that David Lyon is talking about. The practical expression is that these are software systems. These are algorithms that we're talking about. These aren't social security numbers in a paper file in a filing cabinet. It's a highly technical environment.

Mr. Matthew Dubé: I want to give a chance to the other witnesses, but I want to ask my next question just to make sure I have time for it.

It's a great springboard talking about this whole digital element, the software and servers. We talked about foreign states and our relationships with them. It ties into the TPP, for example.

One of the big issues that's been brought up is around localization. In other words, if Canadians have data in the U.S., they have far less legal recourse there than here in Canada, given the U.S. surveillance machine. We know that localization is something that companies in Silicon Valley, for example, aren't particularly fans of. It makes it more difficult for social media and things like that to expand in a way that's beneficial to them.

What do we need to do when we're negotiating trade agreements like this, knowing that goods could be data now as well, and that's something we need to be mindful of? When we see some of these flawed agreements with regard to Canadians' privacy, is that something that needs to be considered in the law?

● (0945)

Ms. Lisa Austin: I'd be happy to comment on cross-border data flows.

This doesn't seem like a Privacy Act issue per se, but I do think we should really understand the issue, again from a kind of constitutional perspective. As a Canadian, if you are physically in Canada and you're living here and residing here, but your data goes to the United States, their position is that you are a non-resident alien—we're in Canada, so we're not resident in the United States—so the fourth amendment of the U.S. Constitution, which provides for protection of privacy, does not apply at all.

There's a lot of Canadian jurisprudence that says that once you're dealing with what happens in a foreign state, it's their rules that apply, not ours, so what you do when you put your data in the U.S., is what I call plunking your data into a constitutional black hole. There's no constitutional right there.

What should we be doing? Data localization is one response to that dynamic. I think it's an unrealistic response to think that this is a solution in the long term. Another response, though, given the size of Canada and the size of our economy, is to negotiate a bilateral agreement with allies like the U.S. to say that when Canadian data is in the United States, you protect us to the same extent that you protect your own citizens.

I would actually go further and say you need to protect us according to our own standards in the Canadian charter, because Canadian charter standards of privacy are better in relation to data in most of these contexts than the American constitutional standards. Why? It's because the Americans still buy into what's called the third party doctrine. They say that if you share information with a third party, such as a telecommunications provider, there's no longer a reasonable expectation of privacy. You've given it up in relation to the States.

It's a crazy doctrine. We've never agreed with it in Canada. The Supreme Court of Canada has denounced it for more than 20 years.

It's crucial, I think, that we actually negotiate and say, “If you want access to our data for any kind of law enforcement or for national security, it's the Canadian charter that applies.” That mimics what the MLAT process tries to accomplish in having the constitutional rights of the data bearer apply, and we need to find a way to do that. I think that's the way forward, but I think it's a treaty that needs to be negotiated.

Mr. David Lyon: I might add, too, that the question suggested some kind of deliberate transfer of data for the purposes of trade or law enforcement or whatever, but in fact data frequently travels through the States between one Canadian location and another. The routing system can take data into the United States and then return it to Canada. This can be even between two locations in the same city, but it goes through the U.S. In those circumstances, the possibility that the individual's information is subject to American law and therefore doesn't have any kind of protection for the individual is true as well. It happens incidentally as data is routed into the United States.

The Chair: That's very, very interesting.

That takes us over your time, Mr. Dubé.

Mr. Lightbound is next.

Mr. Joël Lightbound (Louis-Hébert, Lib.): Thank you all for being here. It's very interesting and much appreciated.

My first question concerns the necessity requirement that we find in section 4 of the act currently, which says that information collected must relate directly to an operating program or activity of an institution.

When we hear that the government has been snooping on the social media of Canadians and millions of records have been data-mined, so to speak, how do you conceive that we should narrow that necessity requirement? Are there specific suggestions you would make to us? What I've read from Mr. Therrien is a pretty broad suggestion. Are there examples around the world that you could point us to as we review the Privacy Act?

I'd start with Madam Austin.

● (0950)

Ms. Lisa Austin: It's a great question. Concerning the necessity standard, I understand why the section 1 framework is the one being suggested. It's a well-known kind of legal framework for proportionality analysis. In international human rights there's a necessary and proportional test as well, which is a great thing to take a look at.

My only hesitation on the necessity requirement is that the section 1 test, if you start to interpret it through the lens of existing jurisprudence, has largely been developed in the context of social legislation. The courts really focus on minimal impairment, and they don't focus on the kind of broader balancing that you would find, for example, in the traditional section 8 of the charter privacy cases. In those search and seizure cases, the “reasonable expectation of privacy” is understood as a kind of balancing. State interests are already balanced against privacy in that provision. Again, the ”reasonable and probable grounds” test is not a minimal impairment test; there is stronger protection for privacy in that kind of balancing.

My only hesitation is not to think that.... I think the necessity test and the section 1 framework are an improvement over what is in the Privacy Act right now, but I'm hesitant about its becoming a kind of stamp of approval for collections, uses, and disclosures, particularly in the context of starting to get into law enforcement or national security, because there is a more robust view of proportionality, I would argue, in section 8 and section 7 of the charter that is not reflected there. It's as if you're jumping to a section 1 justification when you haven't done the more robust analysis early on. I think that's a problem in those contexts.

Ms. Teresa Scassa: The directly related problem with the current standard is that it's too soft and is capable of multiple interpretations. The desire to move to a necessity standard is to try to bring to bear more firmly the concept of data minimization, which is an important data protection principle because it requires a reduction of the amount of information that is collected in the first place. The focus really should be on whether this information is necessary for this program or service. If it's not necessary, then it shouldn't be collected.

Obviously, with any word, there's going to be wiggle room and room for interpretation and room for arguments: “Well, this is actually necessary. because what we're doing requires....” I think this is part of the problem in the big data environment: we start to say that what we're trying to do is collect enough information so that we can do these other analytics or other profiling, which will enable us to do these other things, and therefore it becomes necessary.

I think there are risks with any vocabulary that is used. The goal here is to try to minimize data collection. In combination with other measures being recommended, such as privacy impact assessments and so on, it may be that there are ways in which more supervision can be imposed.

Mr. Joël Lightbound: I want to hear you on another topic. Madam Austin, you've mentioned quite accurately the dangers of information sharing, especially when we think of the Maher Arar saga. Currently Bill C-51 states that the information sharing must be in accordance with current legislation in Canada. In the Privacy Act, we have a general prohibition against the sharing of information in section 8, which is tempered by a lot of exceptions in subsection 8 (2), and it goes on and on. For instance, paragraph 8(2)(b) says that it can be done if it's in accordance with another regulation or law, which is a catch-22, so to speak.

I would like to hear your thoughts on section 8 and hear whether you have any ideas on how we could further narrow the information sharing within the Privacy Act.

Ms. Lisa Austin: One of the big problems is thinking that with Bill C-51, privacy is going to be protected because the Privacy Act applies. The broad authorization for information sharing in SCISA itself seems to capture a lot of what section 8 does. I don't have the act in front of me, but any analysis of this issue has to start from the proposition that compliance with section 8 does not mean compliance with the charter. All sorts of information sharing could be consistent with those disclosure provisions or the use provisions in section 7 or section 8 of the Privacy Act, as it currently stands, yet still violate the charter.

I'm not sure, as a matter of legislative drafting, if you want to change those provisions or just indicate somewhere that in some circumstances this is going to raise charter issues, because it won't necessarily or in all circumstances. The Privacy Act regulates collection, usage, and disclosure of personal information. Not all of that is going to meet a constitutional threshold for the reasonable expectation of privacy. That's the tricky part. When you're contemplating information sharing, particularly in those contexts where the individual is in that coercive relationship with the state, you have to be incredibly mindful that there are charter issues at stake. How can that be built in?

That's why we were arguing that you need an interpretive principle saying that this was meant to be consistent with the charter and build in charter review. Perhaps something could be written into section 8 that this must also be consistent with the charter. You want to build up expertise somewhere of people who understand what the jurisprudence is saying about uses and disclosures of information. When they trigger charter violations, what does that mean? Do you need prior authorization? Is it an issue of safeguards? What do those safeguards mean? Make sure those information processes are compliant from the start so that some person doesn't luck out and find out about this process and then have to go to court 10 years later. You build in charter compliance from the start.

● (0955)

Mr. Joël Lightbound: Seeing that the chair does not interrupt me —

The Chair: If you've got a quick follow-up....

Mr. Joël Lightbound: It wasn't a follow-up; it's another topic.

The Chair: Can we wait until the next round?

Mr. Joël Lightbound: Yes, sure.

The Chair: That concludes our seven-minute round.

We move to Mr. Strahl, please, for five minutes, sir.

Mr. Mark Strahl (Chilliwack—Hope, CPC): Thank you, Mr. Chair, and thank you to the witnesses.

This is a fascinating topic and a fascinating time. Dr. Lyon, people are increasingly concerned about their privacy while they're increasingly revealing more about themselves on a voluntary basis in increasingly insecure media online. Even though they are doing that, you mentioned that people are still cognizant of their privacy rights and expect their privacy to be respected.

I want to speak specifically about one of the recommendations of the Privacy Commissioner. There was a recommendation of a mandatory legal obligation to report serious privacy breaches under the Privacy Act.

Dr. Lyon, do you believe that is a good recommendation, and do you believe that it can be enforced under the Privacy Act?

Mr. David Lyon: It's difficult to answer the second part about the possibility of enforcement. As to the actual revelation about the breaches, it seems to me that it is is essential that we, as a public, know what is happening and when privacy breaches have occurred.

These things tend to be displayed under certain circumstances, but they can also be kept under cover. They can be swept under the carpet so that we never know about them. I think it's essential that we know about those breaches and that they be made public and that there be a requirement to make them public.

As to exactly how you would do that, as I say, I would defer to others.

Mr. Mark Strahl: Speaking of others, Dr. Austin or Professor Scassa, does either of you agree with that recommendation, and do you have any ideas on the best way that those breaches should be reported or on the timeliness of the reporting?

Ms. Teresa Scassa: I would emphasize the importance of two levels of breach reporting, similar to what's been done with PIPEDA.

When the PIPEDA amendments come into effect, you're going to have a first level of breach reporting when breaches reach a certain threshold of harm, and that triggers an obligation to notify both the Privacy Commissioner and individuals who may be facing that potential for harm. That's one level, and it's a tremendously important one, because it's not just reporting the breach but also trying to mitigate harm and notify those individuals who may be affected.

The second level that's in PIPEDA, one which I think is quite interesting, is a requirement for organizations to document any breaches whether they reach that threshold or not, meaning things that are essentially breaches even though the information ultimately didn't end up in anyone's hands. I think that kind of record-keeping and reporting to the Privacy Commissioner doesn't necessarily have to be made open to the broader public—that decision would have to be made—but it could be just reporting to the Privacy Commissioner.

I think it's important because this goes to another thing, which is trying to identify those security practices that are weak and need to be improved within. If the Privacy Commissioner has access to this information, it gives a chance to see whether this is a common problem across government that should be addressed or whether it's a particular department that hasn't adequately trained its staff on certain privacy measures. It allows a more proactive approach to try to address security problems that become visible through this level of reporting.

I would encourage having those two levels so that it's not just harm that triggers notification, but that there's another level where any breach should be reported in order to try to diagnose problems and address them before they become more significant.

● (1000)

Mr. Mark Strahl: Thank you very much.

The Privacy Commissioner also pointed to the Newfoundland and Labrador model as the best model to modernize Canada's Privacy Act. Do you agree with the commissioner, and if so, why? Do you think there are better models, either in Canada or internationally, that we could adopt to improve our act?

Maybe I'll start with Ms. Austin.

Ms. Lisa Austin: My understanding is that this was a recommendation pertaining mostly to the question of order-making power. The Newfoundland model was a hybrid model, and the hybrid model had much to recommend it over an order-making power.

I would say that I don't have a firm view on that particular debate, except that I lean heavily towards the order-making power. I would encourage you, in thinking that through, to take the perspective of the individual rights holder here in terms of privacy, and ask which is going to be better for them in terms of which of these models puts more of a burden on the individual to go to court to vindicate their rights rather than have it dealt with in this other process. We have an access to justice crisis here, and putting burdens on individuals to take it up in court when they are supposed to have these robust rights is, I think, unrealistic. Recommendations from the past that have focused on courts just don't take that into account. That's one thing.

The other thing is that the debate seems to involve a lot of hand-waving and anecdotal evidence. We have multiple jurisdictions in Canada that have different ways of doing this. In Ontario there's order-making power. In B.C. there's order-making power. If there are questions about whether that changes the dynamic by shifting away from an ombudsman model or whether it makes for a more contentious relationship with the government, certainly there are jurisdictions you can get evidence from. This could be a more factually based inquiry. You can take a look at what's going on in those jurisdictions and find that out.

The only other thing I would say is that in these charter contexts that I'm extremely concerned about, having a strong stick is good, because in these charter contexts, the individual is in a conflicting relationship with the state, whereas in the more administrative context, where the state's administering a social program, there's not that strong conflict. There's some conflict, but it's not that fundamental conflict.

I do think that from that perspective, order-making power has a lot to say for it, but I don't have a definitive view.

The Chair: That was a very lengthy answer. It turned a five-minute round into a seven-minute round.

We'll go to Mr. Saini, please, and I'll try to extend the same courtesy.

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

I have one general question, and then I will get to a specific question.

My first general question is that as you know, the government is instituting a computer system called GCDOCS across 17 departments. If one department collects information that they require and need, how do you prevent the other departments from accessing that information about Canadians when it will be on the system for 17 departments to view? Do you have any kind of recommendation?

Ms. Teresa Scassa: I don't think I know enough about the system specifically to know what kind of access is forecast, but there are technological ways, even within a large shared database, that you can create different levels of access for different persons or parties that have access to that database. I'm not sure if one of the measures that is being contemplated is to create those different levels of access to manage access within the database.

● (1005)

Ms. Lisa Austin: I will go back to some of the earlier remarks I made: you can't think of safeguarding privacy just in terms of the administrative processes for sharing information; you have to look as well at the technical systems that we're building. You have to think about it at that level, so that you know how to build those systems and you can put in the safeguards that you should have a legal obligation to have. It's difficult to bolt them on after the fact. It's possible, but it's usually expensive and difficult.

You think about it up front. When you are building processes, you need to think about privacy up front. You think about compliance with the charter up front, and you build it into the technical apparatus that you construct up front.

Mr. Raj Saini: The second question I have is based on national security.

As you know, Canada has many alliances around the world, whether it be the Five Eyes or intelligence sharing with our European partners. I'm wondering if you could give me an idea, because I'm not sure if I understand how it works.

From a foreign government you may have two types of requests. You may have an immediate request when there's an ongoing situation in a foreign country and they need some information on a Canadian, or you may have a long-term request for information on a particular Canadian who is not involved in anything immediately, but could be down the road. How do you analyze that request? More importantly, how do you safeguard the information? Once it crosses a border, that information now is being held in a foreign government's file.

We have the Privacy Act and we have certain safeguards here. How do we ensure that those same safeguards will be maintained in a foreign country, or that the information will not be shared within the departments of that country or sent off to a third country?

Ms. Lisa Austin: That's a great question. I would emphasize the need for safeguards, which is an issue that is coming up in charter jurisprudence. That is partly why we are arguing for an improved accuracy obligation in the Privacy Act itself to set up some obligation to get those assurances.

I think what you need in these alliances and these international contexts is to protect each other's citizens through treaties that agree to extend certain kinds of rights. Then you have audit processes under them, so that people can go and take a look at the information practices. I don't think you can solve that through a privacy act.

Mr. Raj Saini: You would need some sort of super national treaty, because the problem is that each country has a different regime. If we ask them under our regime, another country may have a stronger regime. You would have to create one framework that every country would have to adhere to. Is that something that you're suggesting?

Ms. Lisa Austin: That might be the answer. It might be, at least among allies, that you create some international regime for doing that. I know there's a lot of interest in how to deal with the MLAT process in the evolving world.

There are various models. I don't know what the right one is, but it does seem to me that it's some kind of international agreement, or at least super national in some way. In Privacy Act reform, you can tweak it and start getting at some of these obligations and you can create agreement, but you do need something stronger than that.

Mr. Raj Saini: Mr. Chair, do I have some time left?

The Chair: I'm going to be gracious. Go ahead, please.

Mr. Raj Saini: Let me ask this question to Mr. Lyon, because he has been sitting there patiently and I want to include him in the conversation.

You talked about surveillance. If a foreign country asks us for information, asks us to surveil one of our own citizens, how does that work? Can you give some commentary as to what the process is, what we should be allowing to happen, and what we should prohibit from happening? How should the rights of Canadian citizens be protected, while being a partner to an international country, to make sure that information is still being properly disseminated?

Mr. David Lyon: Do you have a national security or law enforcement regime in mind here? Is that the situation?

Mr. Raj Saini: No.

Let's say a foreign country asks us to surveil one of our own citizens for whatever reason, whether it be a national security question or something else. How do we deal with that? What parameters do we have?

I know Madam Austin mentioned that there's a warrant process, but how do you do that, especially if it's an immediate request?

● (1010)

Mr. David Lyon: This is not an area that I deal with specifically, but it does seem that there needs to be a lot more oversight of the agencies that might be involved in receiving and sharing that information. That seems to me to be a critical issue.

How the actual mechanism would work is not something I'm privy to or know about. It does seem to me, though, that we need a lot more oversight on those agencies that are concerned with law enforcement and security matters, because that's where the issues arise and where things become very murky.

The Chair: Thank you, Raj. Much appreciated.

We now move to Mr. Kelly for up to five minutes, please.

Mr. Pat Kelly: Thank you.

Professor Lyon, in your earlier remarks you mentioned what I took to be a description of a deficiency in understanding all the issues around privacy and how to address them. I think you suggested that we wouldn't be ready yet for a complete overhaul of the act and that there was a substantial need for additional study into privacy matters. I think you even suggested a royal commission of some type, or some type of large-scale study.

Could you identify the things that we don't know? What do we need to research, and what areas require more study before a proper rewrite could be done, in your opinion?

Mr. David Lyon: There are things that we have already been talking about.

In a sense, they can be talked about in terms of technological changes and the new kinds of means of finding out about individuals for one purpose or another. There are things I mentioned in terms of the trends toward a greater use of biometrics, and sensors being embedded in buildings, streets, vehicles, and so on. A lot of it sounds like coming to terms with the technological changes that are already occurring. That seems to me to be crucial.

On the other hand, I've been trying to stress the ways in which the very idea of privacy has altered since the 1980s, when the act was originally conceived. It seems to me to be essential that we bear that in mind as well. This comes into, or is completely consistent with, what Lisa Austin is saying about the need for charter compliance here.

It seems to me that the notion of privacy was once conceived in a very atomistic and individual way, and it had to do with very specific harms that could be identified. In today's situation, we have to think about a much broader range of issues that have to do with democratic participation and human rights, so the very notion of privacy, it seems to me, needs to be expanded.

It's both things: it's coming to terms with the real technological changes—and again, big data is a huge issue here—on the one hand, and it's also understanding how the notion of privacy has itself evolved into a much more social and participatory matter than was thought of in the Privacy Act originally.

Mr. Pat Kelly: Thank you.

In a completely different vein, Ms. Austin could perhaps address this one.

What would be involved in expanding the judicial recourse and remedies under section 41 of the act that the commissioner has recommended? Would implementing this recommendation increase or decrease the expense of staff requirements for the courts? Would this increase or decrease liability settlements and damage costs to the treasury? What would be the net result of that recommendation?

Ms. Lisa Austin: That's the bottom line. You should never ask academics questions about the bottom line.

Mr. Pat Kelly: I might have done that on purpose.

Ms. Lisa Austin: The point about increasing the judicial remedies is that one of the big defects in the Privacy Act that the Privacy Commissioner points to is that the provisions around the collection, use, and disclosure are ones that you can't take to court. You don't have recourse there, yet those are increasingly vital in safeguarding information in all sorts of contexts, whether they be administrative, national security, or law enforcement.

It's absolutely vital that we have something there. Is it going to cost more? Probably, but I would say, again, that recourse an important aspect of protecting privacy rights. Without that, you can't make the Privacy Act work in the context that it's being asked to work in.

● (1015)

Mr. Pat Kelly: I'm not suggesting that cost be a reason not to do it. I just simply wanted an idea—

Ms. Lisa Austin: —what those costs would be. Sorry; I wouldn't know.

The Chair: Mr. Long, you have up to five minutes, please.

Mr. Wayne Long (Saint John—Rothesay, Lib.): Thank you, Chair.

Thank you to our guest witnesses this morning.

I want to start with Ms. Scassa. You were involved, obviously, in the Supreme Court ruling in Ontario. I think it was in January.

Ms. Teresa Scassa: Do you mean the one related to the tower dump?

Mr. Wayne Long: Yes.

Ms. Teresa Scassa: Well, I've written about it.

Mr. Wayne Long: I'll read that comment in a sec.

I'll state this for the committee. I think there's always a balance—and we've talked about this for many months—between liberty and security. Liberty comes with a cost, but it should never be forfeited for security without extreme reasons.

Your quote in an article I read last night basically said that the judge makes it clear that the information that is sought by police should be really limited to the purposes of the investigation. It should not be a fishing expedition.

Recognizing that there's obviously a balance between what the police need to know and a person's privacy, could you elaborate on that case and what happened there in the background?

Ms. Teresa Scassa: This was an interesting case. It came to court because the telecommunications companies involved brought a charter application to court, not because the accused individuals raised charter issues with respect to their rights.

Essentially the police were investigating a jewellery store robbery. They were looking for suspects. They suspected that a cellphone had been used in the commission of the crime, so they sought tower dump warrants, essentially a dump of data from nearby cellphone towers. Rogers and Telus, between them, said this would mean handing over the records of 43,000 individuals who had used their phones within that window of time the police provided, but in addition to that, they sought a great deal more information.

Mr. Wayne Long: For a novice like me, when you say a dump of data, is that basically every bit of information that the cellphone tower picked up through people's phones?

Ms. Teresa Scassa: Well, it was more than that. They wanted to know every cellphone transmission that had gone through the tower. In addition, they wanted the subscriber information linked to those cellphone numbers from the companies, they wanted credit card and billing information, and they wanted to know who those 43,000 people who had just been in that part of the city people were calling,.

After Rogers and Telus pushed back, the police narrowed the scope of their warrants, saying, “Never mind. This is all we want. Now don't take us to court.” They tried actually to get the case thrown out on the basis that they had narrowed the scope of their warrants and therefore the charter issues weren't raised. The court decided to hear it anyway.

It's a very strong decision. In it the court is basically saying that we need guidelines for judges who are issuing these types of orders. The police need to be very careful about what they're searching for. We shouldn't be allowing fishing expeditions. The information sought went way beyond what was required. There should be a different approach to it.

The other thing that the judge said at the end of his decision, about an issue that had been raised by Telus and Rogers, was that once all of this information is in the hands of police after these search warrants are issued and the police collect the information, there are no rules in the Criminal Code, PIPEDA, or any statute as to what happens to that information. Is it kept forever? Is it used for other purposes? Is it just stored in a database somewhere, where there might be a data breach of credit card information and other data?

The judge said this is not for us; this is for Parliament to deal with. The court can't create guidelines around that.

This is an issue if police are going to be collecting huge volumes of information. What happens to it and what are the guidelines around disposal of that information once the purpose for its collection disappears?

Mr. Wayne Long: Ms. Austin, Mr. Lyon, or Ms. Scassa, you can all comment on this question if you want.

Commissioner Therrien recently was critical of calls by RCMP Commissioner Bob Paulson and the Canadian Association of Chiefs of Police for, basically, a new law that would expand the right for police to have warrantless access.

Mr. Lyon, can you give me some comments on what you think about that?

● (1020)

Mr. David Lyon: There has been a requirement for warrants for many years, and this requirement has been seen as essential to maintaining the integrity of the individual's privacy.

It seems to me that gaining access without a warrant to people's personal information in the pursuit of law enforcement or for any other purpose is simply unacceptable. It's something that needs to be written into our legal system. We need to know that there is a clear warrant for every access to personal information.

The Chair: That takes us up to the five minutes.

We're going to have a little bit of time at the end of the meeting if anybody still has a question. I know Mr. Lightbound had a question he wanted to put.

In order to finish off, we have Mr. Dubé for three minutes.

[*Translation*]

Mr. Matthew Dubé: Thank you, Mr. Chair.

I would like to go back to the way in which offenders are punished. When I look at the recommendations, unless I am mistaken, I see only one that really deals with the kinds of possible consequences in cases of breach of privacy. It reads: “Expand judicial recourse and remedies under section 41 of the Act.”

Transparency is also mentioned a lot. It is essential, no question. It is about making it mandatory for privacy breaches to be declared and to educate the public. All those things are essential, no argument from me.

In your opinion, what should be the consequences for the offenders, if I may put it that way? We are talking about telecommunications companies, even governments or police forces on occasion. Canadians can actually be as equipped and informed as you like, but if those people are in no real danger of facing any consequences, the act is somewhat lacking in teeth.

[*English*]

Ms. Teresa Scassa: That's a complex challenge. Right now there are class action lawsuits already under way against the federal government for negligent handling of personal information, for data breaches. Civil recourse and class action lawsuits are going to become more common, so that is one way in which people can have their day in court.

Professor Austin has talked about charter recourse, and there is charter recourse that's available. In some cases it can be brought by the affected individuals. We were just speaking about a case in which it was brought by telecommunications companies that felt that too much data was being sought from them, and that is not the only case in which companies have pushed back. There are these other recourses that are outside the Privacy Act.

In terms of the Privacy Act itself, one concern is exposing the government to liability. If you create obligations or standards that are set in very strong terms in the legislation, that may increase the risk of liability for the government.

In part, the model has also been one of attempting to improve compliance and improve practices within government around personal information. On one level, that's been the ombudsman model. Now the commissioner is seeking additional recourse, an additional means for citizens to insist on compliance with their rights.

Whether that involves just getting a court order for recommendations to be enforced and practices to be changed or whether that also includes a right in damages is not entirely clear, because you can have a recourse to have a court order, a change in practice, without having recourse to get damages. Whether it's required is something to consider.

[*Translation*]

Mr. Matthew Dubé: Allow me to focus your answer, because I do not have much time.

With the government, I understand. However, with telecommunications companies and banks, for example, there is less need to be concerned, because they have to comply with the law 100%. With the government, I can see that a slight twist is needed.

Mrs. Teresa Scassa: Banks and telecommunications companies are subject to the Act respecting the protection of personal information in the private sector. In those circumstances, I believe that there is a way to improve recourse under that act.

Ms. Austin raised one of the problems: the burden that the individual must bear. The cost of going to court is very high, of course. We see very few people going to federal court to try and obtain damages under the Act respecting the protection of personal information in the private sector. I even believe that people are representing themselves in court, because having the services of a lawyer is too expensive. That is another problem.

● (1025)

Mr. Matthew Dubé: I understand.

Thank you.

[*English*]

The Chair: Perhaps this would be a conversation if we had a review of the PIPEDA legislation, but I appreciate the sentiment.

Colleagues, I always like to make sure that every member of Parliament at the table has an opportunity to ask questions. There are two members of Parliament here who have not been able yet to engage in the conversation.

Mr. Scarpaleggia or Mr. Picard, did you have a question?

Mr. Francis Scarpaleggia (Lac-Saint-Louis, Lib.): Yes, but I will....

[*Translation*]

Mr. Michel Picard (Montarville, Lib.): Thank you, Mr. Chair.

My thanks to the witnesses.

I am going to submit this to you and I would like your comments. I will limit myself to one question.

Information in general is evolving. The quality of the information gathered changes according to the context in which it is received and used. Very often, the content itself is not really important, with exceptions like the social insurance number, of course.

If I give my name and my date of birth, for example, I open myself to some vulnerability in some areas. At the same time, if I subscribe to a birthday club so that I get a letter each year, I must also provide my name and my date of birth. So I have just made public information that could have been dangerous to reveal in another context.

Given the development that Mr. Lyon talked about, who is going to decide the circumstances in which too much information is being gathered?

[*English*]

Mr. David Lyon: It really depends on what other uses are made of that information.

The question about big data has already been raised several times, and that seems to me to be crucial here, because there are many bits of information about us that are far more trivial than our birthdates, and they can be used, once they are concatenated with other data, to create a profile of us so that we end up with profiles that exist within both corporations and law enforcement and national security agencies that are fictions, in a sense, because they are a creation from tiny fragments of data collected from all over.

That, it seems to me, is an issue we really have to address within any attempt to revise these laws.

Mr. Michel Picard: I totally agree on the usage issue.

Ms. Austin, you mentioned something about limiting agencies to collecting information that corresponds to their specific needs, no more and no less. With the evolution of information, how do I evaluate what seems to be within my mandate?

Ms. Lisa Austin: Do you mean in terms of questions of data minimization?

Mr. Michel Picard: I come from the intelligence community, and the fun of analyzing intelligence is not to get it but to put it into context.

All of a sudden, I may start to look at people who don't have any hair, for no reason. It doesn't mean anything. Why should I know that? I don't know. Maybe in another context I will link that with something else, and oh, that's interesting. I have a profile of an individual who fits this image. All of a sudden, the no-hair issue becomes a very hot issue, and it may exceed, at some point, the mandate I have in my agency.

Who is the judge of evaluating where I stop gathering information, or whether I should stop?

Ms. Lisa Austin: That is a great question. I guess I would just add one additional way to think about it.

There is the upfront way of thinking about it, but maybe we also need to start thinking about how to review the practices of different departments. I imagine they would have their own norms. Yours would be very different from some other government agencies. After the fact, how effective are these practices?

We might not know up front, and maybe we need to give the benefit of the doubt in certain circumstances. That is a different question. Surely we need to be building on after-the-fact accountability and review to say, "Well, what have you been doing? What has it allowed you in terms of effectiveness?" If it is not effective, maybe we need to go back and change those practices rather than letting them go on.

When it is difficult to know ahead of time, maybe you need to start thinking about some models that combine an initial discretion with the knowledge that you are going to be held to account for what happens here, and we are going to review it.

● (1030)

The Chair: In the interest of making sure everybody else gets their questions, at about five minutes left, I need the committee's time for about 10 minutes to discuss future business.

Francis, do you have a quick question?

Mr. Francis Scarpaleggia: I'm just looking for affirmation of whether my understanding is correct.

We have an Access to Information Act, which was probably a very prescriptive thing. The government could only have access to certain information. For tax information, for example, it was social insurance number and address. Then as technology expanded, other information was available—IP addresses, for example. Even technology that already existed all of a sudden became relevant. Hydro meter readings are an example, because of grow ops and so on.

Is my understanding correct that essentially the act is out of date because it doesn't take into account all this new information that is available, and that somehow we have to codify what we should be allowed to collect? In fact, we'll always be a step behind, because the technology will always be expanding. To fill those gaps, we'll have to rely on court decisions until we have enough information to amend the act again to deal with things like metadata and so on. Is that a correct way of looking at the process we're involved in here?

Ms. Teresa Scassa: I would almost say the act is out of date because it's the act. In a sense, in our conversation today we've moved between the private sector legislation, the national security establishment, the charter, and the Privacy Act, and references have been made as well to the fact that this whole paradigm has changed. To address some of these issues in their specific silos—this is a Privacy Act issue, this is a Criminal Code issue, this is a national security issue, this is an access to information issue—may simply be an out-of-date approach overall.

Mr. Francis Scarpaleggia: We're really trying to pinpoint what should be acceptable and what shouldn't be acceptable, but we can never be up to date on that. Is that correct? Is that a way of looking at it?

Ms. Teresa Scassa: I think that's right. It is constantly changing, but it may just be that the paradigm in which we are structuring these issues also needs to have some reworking and rethinking.

Mr. Francis Scarpaleggia: The rules that we use to make those decisions can be—

Ms. Teresa Scassa: It's the rules, and it's also the way that we separate issues and say this is this kind of issue, and that's the other kind of issue. The questions of algorithmic governance that Professor Austin has raised also raise really interesting issues about human rights that go beyond just the human right to privacy but also extend into other types of human rights. That's part of the challenge as well.

Mr. Francis Scarpaleggia: We will always have to rely on jurisprudence, to some extent, to decide what is acceptable and what is not acceptable. The act can never be up to date in that respect. Is that correct?

Ms. Teresa Scassa: I think that's right.

The Chair: I'm not quite so pessimistic. We can always write it in a way that allows for dynamic systems.

I know Mr. Long and Mr. Lightbound each have a question. We'll go to Mr. Lightbound first.

Mr. Joël Lightbound: I'll be very quick, and it's more or less a yes-or-no question. My question is for Mesdames Scassa and Austin.

As far as I know, metadata is not defined anywhere in Canadian legislation. Correct me if I'm wrong, but I don't think it is. Do you think it should be included in our definition of personal information in the Privacy Act, so that it becomes protected, or that there should be something about it in the Privacy Act?

Ms. Teresa Scassa: I was just going to ask what you mean by metadata, so obviously the answer is yes. It's actually quite a broad term.

Mr. Joël Lightbound: It is. That's true.

Ms. Teresa Scassa: It's basically information about information. In any event, yes, I think probably that would be the case.

Ms. Lisa Austin: I think it would be helpful under the definition of personal information, which is broad enough to capture it. It's identifiable information, so in many contexts metadata would definitely fit as identifiable information. It would be helpful to clarify it by saying, "for instance, it includes...", and when you have the non-exhaustive list, to put that in. It's interpretatively helpful.

The caveat then is how you define metadata. If you used some kind of general thing, such as "this includes information about information", or something like that....

● (1035)

Mr. Joël Lightbound: That's all.

Thank you.

The Chair: Thank you very much.

Mr. Long, do you have a quick supplementary question?

Mr. Wayne Long: It's not that quick, so I'll just save it for the future.

The Chair: The chair has one quick question for Ms. Scassa.

In your presentation, you talked about indirect collection of data from the private sector by the government, unbeknownst to the rest of us. My personal information, which would normally be governed by PIPEDA in a relationship that I would have with a private sector company, could then, through a relationship that the company has with the government.... Did I hear you right?

Ms. Teresa Scassa: It's just that PIPEDA permits companies, without the knowledge and consent of the individual, to disclose information to investigative bodies, police, law enforcement, national security, or other regulatory bodies upon their request. The company can refuse to do so without a court order, but they can make these voluntary disclosures. That has been a significant issue under PIPEDA, under which information can be voluntarily disclosed, without a warrant, to government actors, essentially.

The Chair: Okay.

I have one quick question for you, Ms. Austin. It deals with jurisprudence.

We talked about sovereignty issues as they pertain to data. Mr. Saini actually had a line of questioning on this. The courts decided years ago that any person who enters the territorial confines of Canada is granted all of the privileges and protections that a Canadian citizen is afforded. Has there been any jurisprudence or any test put to whether or not a person's information or their personal data, if it enters the jurisdictional boundaries of Canada, has the personal protections afforded by the Charter of Rights and Freedoms?

Ms. Lisa Austin: To my knowledge, that issue hasn't been litigated.

The Chair: It hasn't been tested yet.

Ms. Lisa Austin: Not to my knowledge; when your body's in one place and your data's in another, you are sort of in an unknown area.

The Chair: Okay. Thank you very much.

Mr. Lyon, my question for you comes from the example you gave me, as a former IT professional, when we were talking about information moving from a hub in Canada to a hub in the United States and then back to potentially the same city in Canada. The data packets, which is what I assume you were talking about in a network transfer, would potentially be routed through a jurisdiction outside of Canada in order to get to their destination. That raises some questions.

Would you have any witnesses you could propose to this committee who could speak to the IT components of this issue? That's some fairly technical stuff that we'd have to get right. I would love to have a line of questioning with somebody who could answer some highly technical questions.

Mr. David Lyon: It's tremendously important that you do. The person I'd suggest would be Andrew Clement at the University of Toronto.

The Chair: Okay. Thank you very much.

On behalf of my colleagues, I thank you all for your testimony here today. If there's any information that you want to follow up on, please provide it to the clerk of the committee. We may call upon you for clarification at some point in time as we go through the Privacy Act. Thank you very much for your time.

Before you go, colleagues, I want to discuss a bit of committee business. Do you want to do this in a public meeting or do you want to do it in camera? We can move in camera in a second if you want to. It's up to you. I want to discuss the schedule and the witness lists we have coming up for the next couple of weeks.

An hon. member: I would say in camera.

The Chair: We'll go in camera? Okay. We'll suspend and go in camera.

Again, thank you very much, witnesses.

[*Proceedings continue in camera*]