HOUSE OF COMMONS
CHAMBRE DES COMMUNES
CANADA

44th PARLIAMENT, 1st SESSION

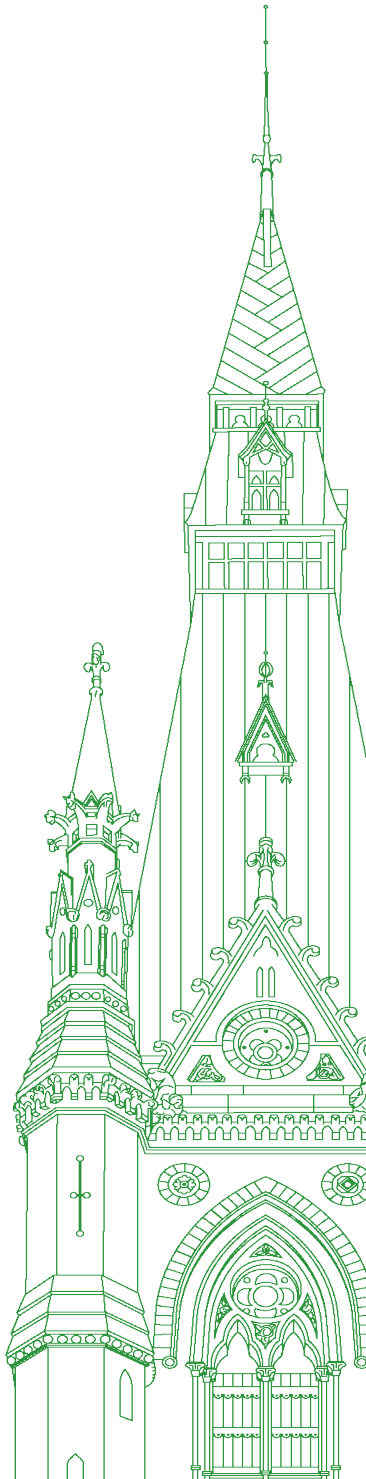
Standing Committee on Access to Information, Privacy and Ethics

EVIDENCE

NUMBER 024

PUBLIC PART ONLY - PARTIE PUBLIQUE SEULEMENT

Thursday, June 2, 2022



Chair: Mr. Pat Kelly

Standing Committee on Access to Information, Privacy and Ethics

Thursday, June 2, 2022

● (1550)

[*English*]

The Chair (Mr. Pat Kelly (Calgary Rocky Ridge, CPC)): I call this meeting to order.

Welcome to meeting number 24 of the House of Commons Standing Committee on Access to Information, Privacy and Ethics. Pursuant to Standing Order 108(3)(h), the committee is studying the subject matter of main estimates 2022-23.

I would now like to welcome our witness today, Mr. Daniel Therrien, Privacy Commissioner of Canada. Not to pre-empt any of his remarks, but I will point that he will be leaving his office for retirement shortly. This will be our last opportunity to have him at committee. I thank him in advance for his long service to Canada and to this committee.

With that, we'll leave it to you, Mr. Therrien, to begin your remarks.

Mr. Daniel Therrien (Privacy Commissioner of Canada, Office of the Privacy Commissioner of Canada): Thank you very much, Mr. Chair. That is very kind.

[*Translation*]

Good morning, Mr. Chair, and members of the committee.

Thank you for the opportunity to appear before you today to discuss some of the lessons of the last eight years and some high-level recommendations on how the law should be reformed.

We are living in the fourth industrial revolution, the digital technology revolution. These technologies are disruptive.

As the pandemic has shown, there can be several benefits to this, for instance in health and education, or even the environment. Digital technologies can indeed serve the public interest.

We have also learned over the years that the consent model means of protecting privacy has serious limitations. It is neither realistic nor reasonable to ask individuals to consent to all possible uses of their data in today's complex information economy, for instance in some circumstances where artificial intelligence is used. The balance of power is too unequal and the asymmetry in terms of who controls personal information is too great.

In fact, consent can be used to legitimize uses that, objectively, are completely unreasonable and contrary to our rights and values. And refusal to provide consent can sometimes be a disservice to the public interest.

During my term, however, we have also seen through investigations that these technologies can present not just potential risks to privacy, but also cause real harms.

For example, our Clearview AI investigation showed that the company used facial recognition technology in a way that amounted to mass surveillance. And our investigation into the RCMP's use of the Clearview technology demonstrated the growing risks posed by public-private partnerships and the absence of a legal framework governing the use of such sensitive biometric data.

The Cambridge Analytica scandal, studied by a committee composed of members of the Standing Committee on Access to Information, Privacy and Ethics and legislators from other countries, showed that privacy violations could lead to violations of democratic rights.

Finally, our investigation into Statistics Canada revealed that a government institution believed evidence-based policymaking could justify the collection of line-by-line financial records of citizens, another form of surveillance.

This leads to the following conclusion. While disruptive technologies have undeniable benefits, they must not be permitted to disrupt the duty of a democratic government to maintain its capacity to protect the fundamental rights and values of its citizens.

What we need, then, is real regulation of digital technologies, not self-regulation.

The previous Bill C-11 would unfortunately have allowed more self-regulation by giving companies almost complete freedom to set the rules by which they interact with their customers, and by allowing them to set the terms of their accountability.

[*English*]

If we draw on the lessons of the last few years, we will adopt private sector privacy laws that will allow for innovation—sometimes without consent—for legitimate commercial purposes and socially beneficial ends, within a framework that protects our values and our fundamental rights.

In the public sector, we also need laws that limit the state's ability to gather information about its citizens beyond that which is necessary and proportional to achieving its objectives.

Overall, we need federal laws in the public and private sectors that are rights based, that have similar and, ideally, common principles for both sectors, which are based on necessity and proportionality, which are interoperable at both the national and international levels and which give the regulator the power to audit and enforce that it needs to ensure compliance.

Adopting adequate privacy legislation is not sufficient in itself. The regulator must also have adequate enforcement powers, be properly funded and be given regulatory discretion to manage its workload to ensure that it can protect the greatest number of individuals effectively within limited resources.

In July, the Privacy Act extension order will come into force, giving foreign nationals abroad the same right as Canadians to request access to personal information about themselves that is under the control of federal government institutions.

The government believes that this will result in a large increase in the number of requests for access, which will trickle down by way of complaints to our office. The OPC has communicated its funding needs to the government. To date, no new funding has been provided. This is a critical issue for the OPC as it requires additional funds to perform these newly mandated duties.

As for the broader financial impact of law reform, we believe, based on the experience of other data protection authorities, that our budget would need to double, approximately, if the promised new law for the private sector were similar to the former Bill C-11. We also anticipate the expansion of advisory functions and the obligation to review industry codes of practice.

We welcome these new responsibilities as they would promote compliance with the law when programs are at the design stage. Nonetheless, we are concerned that the non-discretionary nature of these activities and of our investigative work would deprive us of the ability to risk-manage our caseload and give greater priority to matters of higher risk. We therefore urge you, when a bill is eventually presented to Parliament, to give my office greater discretion to manage our caseload by selecting its advisory and investigative files to ensure that we can protect the greatest number of Canadians effectively within our limited resources. Not only would this allow us to operate more efficiently, but we have also estimated that it would result in a cost saving of nearly $12 million per year.

As for enforcement powers, I have consistently called for quick and effective remedies, including the power to issue orders and to impose significant monetary penalties proportional to the financial gains that businesses can make by disregarding privacy. Yet further evidence of the need for these powers was provided yesterday with the result of our investigation into Tim Hortons.

Like many other data protection authorities in Canada and abroad, the OPC should also be empowered to conduct proactive audits to verify compliance with the law. The need for this was demonstrated in spades in the recent story about the Public Health Agency's use of mobility data that was obtained in modified form from private sector organizations. In a world where innovation requires trust, an important factor of trust in the population would be the assurance that an independent expert has their back, will verify and ensure compliance with the law and will take appropriate action to stop or correct non-compliant behaviour. Again, these are powers or authorities that a number of our provincial colleagues have in Canada and that a number of our international partners have, including in common-law jurisdictions such as the United Kingdom.

I would like to leave you with a few final thoughts on the future of privacy laws federally and their interoperability with the laws of other jurisdictions, both domestically and internationally.

Domestically, we see that Canada's three most populous provinces have made recent proposals towards responsible innovation within a legal framework that recognizes privacy as a fundamental right. Quebec adopted such a law in 2021.

All of these provinces confer order-making powers on data protection authorities, and they propose to give them the authority to impose monetary penalties directly without going through an administrative appeal—but subject to judicial review. We ask for similar powers, in part so that all Canadians, regardless of their jurisdiction, have access to quick and effective remedies if their privacy rights are violated, and in part to ensure that the OPC remains an influential and often unifying voice in the development of privacy in Canada. If the powers of provincial and the federal authority are different, if the process federally is longer than that in the provinces, I'm concerned that citizens will address themselves to provincial authorities and that the influence of the federal authority will become less.

● (1555)

[*Translation*]

Globally, it is also essential that Canada's laws be interoperable and not too different from international standards. Some industry stakeholders say that a made-in-Canada approach has been good for the country and that a rights-based approach would hurt innovation.

The idea that rights-based law would impede innovation is a myth. It is simply without foundation. In fact, the opposite is true. There can be no innovation without trust, and there is no trust without the protection of rights.

In our view, a made-in-Canada approach that would be too different from what is becoming the international gold standard would not be in the interest of Canadian business. To the contrary, interoperable laws are in Canada's interest.

In closing, my message to this committee is this: continue the work that you and your predecessors have been doing on these important files. As legislators, you have the power to bring meaningful change to our privacy regime and your reports to date point in the right direction.

Remember also that our laws should protect the right to privacy in its true sense: freedom from unjustified surveillance. Thus, legislation should recognize and protect the freedom to live and develop independently, free from the watchful eye of the state or surveillance capitalism.

In other words, the law should protect our values and rights, hard won over centuries, and should not be set aside in order to benefit from digital technologies.

It has been an honour working with all of you. Thank you for the extra time this afternoon.

I am happy to answer any questions you might have.

● (1600)

[*English*]

The Chair: Thank you, Commissioner Therrien.

Yes, indeed, to the members who have been wondering, yes, I allowed him whatever time he needed to make his opening statement.

With that, I want to just have a quick word about how I plan to proceed with this meeting.

We started a little bit late. I want to go through our normal first round of six minutes each. The second round, which is Conservative and Liberal; then two and a half minutes each to the Bloc and the NDP; and then back to five minutes to the Conservatives and Liberals. That would take us to about 4:50 p.m.

I propose to do a third round if there is appetite for it. If there is not, we can suspend at that point. If there is appetite, we can continue through and should have enough time to get a third full round in and then allow for a few minutes of committee business at the end when we have some housekeeping items that need to be addressed.

I'll be vacating the chair for a portion of that time to speak in the House, but I will be back in time to take over the short committee business portion where, as I said, we have some housekeeping to take care of.

We'll try to get people out. I know there are people with flights tonight, too.

With that, Mr. Kurek, you have six minutes.

Mr. Damien Kurek (Battle River—Crowfoot, CPC): Thank you very much, Mr. Chair.

First, let me thank you, Commissioner, for your work over the last number of years and for your service to Canada. Congratulations, and I hope you are able to enjoy your upcoming retirement.

Commissioner, I'm curious, and perhaps I could ask a very broad question first on whether or not you believe that the whistle-blower protection laws in Canada are adequate.

Mr. Daniel Therrien: That has not been a matter that we have experienced or applied very frequently. There are provisions in privacy laws that protect whistle-blowers who wish to make complaints, for instance, either against a company or a government institution. They are used extremely rarely; in fact, I do not recall a case. I would not be able to speak from experience on that matter.

Mr. Damien Kurek: Thank you, Commissioner.

I know there is an ongoing investigation of a leak of some information from the CRA.

Could you share with this committee if you have any recommendations as to how to ensure that whistle-blowers could be protected to ensure that when information is brought forward in the public interest, those who might be bringing it forward will not face repercussions?

Mr. Daniel Therrien: In broad terms—and I have not looked at the Privacy Act or PIPEDA in that regard recently—obviously a whistle-blower should be protected. Their identity should be protected by the tribunal or the office that considers their complaints. At the same time, the complaint needs to be examined in a fair way towards the institution or organization being investigated.

However, I would not have anything really to say other than obviously the identity of the complainant, who is a whistle-blower and for whom there may be reprisals, should be protected.

Mr. Damien Kurek: Thank you, Commissioner.

I'm curious. With Bill S-7 currently before the Senate, an act to amend the Customs Act and Preclearance Act, have you had a chance to examine this piece of legislation and give advice on it?

Mr. Daniel Therrien: I have, and officials of the OPC will testify on Monday before the Senate on this legislation. We have prepared for it, so I can say a few things.

Clearly, one of the areas of activity we've examined and investigated during my mandate has been this issue of the searches of cellular devices or electronic devices at the border. There is no question that privacy interests at the border are lesser than within the country itself, which gives more latitude to border officers to search luggage, persons and electronic devices.

We have, in our investigations, underlined the fact that a cellular device or an electronic device is not the same as luggage or a piece of mail. There is much more very sensitive personal information contained in an electronic device. Therefore, although we're at the border, the privacy interests of information found in an electronic device mean that these devices cannot be searched without any grounds whatsoever.

The courts have agreed with that—

● (1605)

Mr. Damien Kurek: Sure.

Mr. Daniel Therrien: —leaving to Parliament the authority or the choice to craft a reasonable standard for border officers to perform their duties.

I would simply end by saying that I know that Bill S-7 proposes a novel standard to authorize border officers to perform their duties. At the end of the day, I would say that it seems to me that no standard will stand up before the courts unless there is an objective basis for the belief by a border officer that he or she will find material that is unlawful. Because of that, I'm not so sure a law can have a standard below reasonable grounds to suspect, which is a known standard, because the courts, it seems to me, will inevitably require some objective basis on the part of the border officer to perform the search.

Mr. Damien Kurek: I'll ask in the few seconds I have left: Do you believe that the bill, as written, is then problematic in terms of not creating an appropriate threshold?

Mr. Daniel Therrien: There is an attempt in the bill to respond to a court decision and craft a standard. I have heard operational issues at the border, but I have not heard arguments or evidence yet that would address the question I am raising, which is that it seems to me the courts will require an objective basis. I have not heard that evidence on the part of the government yet. It may exist, but I have not heard it yet.

Mr. Damien Kurek: Thank you, Commissioner.

The Chair: Thank you.

Now for six minutes we have Ms. Saks.

Ms. Ya'ara Saks (York Centre, Lib.): Thank you, Mr. Chair.

I would like to thank Commissioner Therrien.

It's good to see you again and to thank you in person for your service to Canadians and to all of us as parliamentarians. As an agent of Parliament, your role is really to oversee compliance with the Privacy Act and also to promote the privacy of Canadians in the work we do in many spaces.

In my short time here in Parliament, the digital space is one that has grown. It is being used in every part of our lives through these phones, particularly during COVID. As our workplace environments have become our home environments as well, issues of privacy have certainly been elevated in many aspects of our daily lives.

The Minister of Justice was mandated to develop amendments to the Privacy Act. I'd like to ask you if you support the work and what changes he should prioritize as you exit your years of service.

Mr. Daniel Therrien: The Department of Justice published a consultation paper about a year ago on potential principles for a new public sector law. We recommended certain changes, but by and large, we were fairly happy with the general tenor of the bill and its principles.

One of the issues, if not the main issue, parliamentarians should think about when they consider public sector law is the growing use of technology. There is much greater ease with which both companies and government departments can collect information, so it is important to ensure that technical ease is controlled by rigorous standards. The international norm in that regard is necessity and proportionality. I think that is the main point to be made with respect to the Privacy Act.

● (1610)

Ms. Ya'ara Saks: Thank you for that.

I'd like to step up on that, if I may. You recently collaborated with five other countries to advance privacy in video conferencing and teleconferencing software. Can you explain what this means for ordinary Canadians, particularly in this new Zoom world? Even today, we have members of our committee who are video conferencing with us.

Mr. Daniel Therrien: That's an interesting question. It speaks to the role, among other things, of the OPC, not only as an investigative body but also as a body that can provide advice to companies or departments on how to comply with privacy laws.

That exercise involved, as you said, five data protection authorities across the world. The U.K. was one of them, as well as us. Because of COVID and the greater use of platforms like Zoom, Microsoft Teams and the like, these platforms were extremely helpful if not necessary for people to communicate and work, and so on. There were certainly issues, if not concerns, as to whether these platforms properly protected the personal information of users. Rather than formally investigate whether the platforms complied with the law, we had a more informal engagement with a number of these platforms where we were shown some of the technologies being used and how they were used, and we provided certain advice to improve privacy protection.

That exercise did not lead to a stamp of approval by data protection authorities. We looked at everything. We thought everything was compliant with the law, but we thought it was still useful to have this engagement with these companies to see whether anything clearly awry was happening, which we did not see, and to try to elevate the level of privacy protection in the use of these technologies.

Ms. Ya'ara Saks: That's a really important point. The privacy of employees working from home, particularly through these platforms, is something that's certainly of national concern to Canadians. It's something that we've even discussed here as a potential motion for a study by this committee. Sadly, not all of my colleagues agreed with that.

Do you think it's important that we do an exploratory search of this? If this is going to be the technological norm for our employees, both in the public and private sectors going forward, employees need to know that their privacy is protected in the relationship with their employers when they are engaged on these platforms and this technology is a requirement of their work.

Do you have thoughts about that?

Mr. Daniel Therrien: It's certainly an issue that needs to be examined. There may be jurisdictional issues as to whether this falls under provincial or federal jurisdiction. I will not say it is clearly not under federal jurisdiction. There are companies under the ambit of PIPEDA, the private sector law, that play a role in that sector, so I'm not saying, "Don't go there", but if you go there, which is certainly a worthwhile issue to examine, ensure there is federal jurisdiction.

Ms. Ya'ara Saks: Yes or no, would a study be worthwhile on this issue?

Mr. Daniel Therrien: Yes, on the substance.

The Chair: Thank you.

Now Mr. Lemire.

[*Translation*]

Mr. Sébastien Lemire (Abitibi—Témiscamingue, BQ): Thank you for welcoming me to the committee, Mr. Chair.

Mr. Therrien, let me start by thanking you for your work throughout your career.

I usually sit on the Standing Committee on Industry and Technology, where you have appeared in the past.

I consider your testimony something of a legacy. It includes a number of elements, and I will become the messenger to see that all your recommendations are implemented, in particular regarding our role as legislators and the need to double your office's budget to improve its effectiveness in the face of "surveillance capitalism", which is a great term.

That said, regarding the federal government's use of mobility data, the government did inform you of its intentions, but it also chose to use other experts to look into technical ways of depersonalizing the data. In the end, there have been times during your mandate when you might have felt superfluous. At least it seems that way.

Were there times when you felt sidelined by the government?

● (1615)

Mr. Daniel Therrien: It was not the dream of certain companies or departments to be investigated by the Privacy Commissioner, and I understand that. In the case of the mobility data, the government used experts. It was not legally required to consult us on the details.

To my mind, the basic issue is that citizens do not have the information they need. In any event, the rules governing the use of technology and information are so complex and the contracts are so complicated that we cannot expect that the normal and usual course of action for a consumer with a potential problem would be to lodge a complaint with my office.

That leads us to proactive audits. In my opinion, proactive audits would be very helpful in restoring trust in government and companies as to the use of mobility data. They are already conducted in other countries, and even in some Canadian provinces. They would allow the commissioner's office to verify compliance, or in other words to guarantee citizens that their data is being used correctly. From time to time, the commissioner's office could conduct specific audits to ensure that, in a given sector or company, the information that the company or department says it is using in accordance with the law is indeed being used that way.

Ultimately, what the government did was legal under the current act. In my opinion, however, it did not inspire a great deal of confidence in citizens and consumers. The commissioner's office needs the tools to conduct these proactive audits. They should not be broad or seek to examine all commercial or government activities. Rather, they should evaluate the risk and the environment to ensure that certain practices that might be problematic for the public are subject to investigation. In addition, the concerns would have to be confirmed, in which case the commissioner's office could recommend or, better yet, order changes, or confirm that everything was done correctly. That would inspire public trust.

Mr. Sébastien Lemire: Indeed. As you know, the RCMP obtained licenses from Clearview AI. Allow me to quote your report of February 2, 2021:

> In addition, we have determined that Clearview has collected, used and disclosed personal information of individuals in Canada for inappropriate purposes that cannot be justified by obtaining consent.

Can we say that the RCMP was negligent or in violation in its use of facial recognition technologies?

Mr. Daniel Therrien: I would not say negligent. I have pointed instead to public-private partnerships. The government and its institutions are increasingly calling upon private companies that have developed technologies—which is normal—to help government carry out its programs. In this case, it was the RCMP.

It is normal for a federal government institution to call upon the private sector, but in so doing it must not be able to use data that it could not collect itself. Violations of laws cannot be subcontracted to the private sector.

In this case, the company clearly violated the law applicable to the private sector, that is PIPEDA, or the Personal Information Protection and Electronic Documents Act. The RCMP called upon this company, which violated the law.

In our opinion, a reasonable interpretation of the law for the public sector, which governs the RCMP, is that it should have verified the legality of the company's practices, which it hired by contract. This applies to the RCMP, but equally to all government departments.

● (1620)

Mr. Sébastien Lemire: Quite right.

Thank you, Mr. Chair.

[*English*]

The Chair: We now have Ms. Collins for six minutes.

Ms. Laurel Collins (Victoria, NDP): Thank you, Mr. Chair.

I also want to thank Mr. Therrien for all the work he's done. I remember the Harper government's Bill C-51 in 2015. I so appreciated your criticism and commitment to upholding Canadians' privacy rights. That has been ongoing. Thank you for your service.

In your departmental plan, you indicated that your office is reviewing potential structural and operational changes. Can you describe what changes you're considering and what impact they might have?

Mr. Daniel Therrien: I'll be glad to do that.

As I recall, Bill C-11 was tabled in the fall of 2020. The government has announced that a successor will be tabled in 2022, perhaps before the summer.

I thought it was important that the OPC start thinking about how it would be organized to inherit new responsibilities that the earlier Bill C-11 would have given the OPC. We don't know what the new bill will say, but there's a chance, of course, that it will have many elements of Bill C-11. The idea is to get ahead of the curve and think about how we would exercise these responsibilities, so we're not caught off guard if the transition period after the adoption of the bill is shorter than we would hope.

Among the responsibilities that Bill C-11 would have given the OPC—and we think it's likely this will continue to be the case—is order-making. It would be subject to appeal before a tribunal, which we think is unnecessary...but still order-making. That would require, we think, the setting up of an adjudication branch of arbiters or adjudicators. Right now, we have investigators who make recommendations, but with new legislation that has order-making powers, we would likely need to have adjudicators somewhat distant from investigators to ensure the fairness of processes.

That is one area we looked at.

The bill also provided for a review function of the code of practice.

We have looked at all the new authorities Bill C-11 would have given the OPC, and we have given some thought to how we would exercise these responsibilities.

Ms. Laurel Collins: Thank you so much.

You also mentioned that, in July, foreign nationals abroad are going to have the same rights as Canadians in terms of their ability to request access to personal information.

Can you explain how the extension order will impact the operations of your office, and how much of an increase in complaints you expect to receive as a result?

I will then have some questions about budgets.

Mr. Daniel Therrien: I'll start by explaining what the current law is.

The Privacy Act gives Canadian citizens the right to access personal information about themselves held by the government. That right does not exist for foreign nationals, except when they proceed through Canadian agents—

Ms. Laurel Collins: Just because we're quite short on time—we have about a minute—do you want to...?

Mr. Daniel Therrien: To cut this short, the government expects that there will be a very significant volume of access requests by foreign nationals, some of them immigrants interested in their immigration status, and proportionally there will be an increase of complaints with the OPC. We think there will be an important resource demand for the OPC. We have made a request to the government, which has not been denied. It's under consideration. We think it's really important to receive funding for this activity.

Ms. Laurel Collins: You have stated that you communicated your need for increased funding to the government, yet no new funding was provided.

● (1625)

Mr. Daniel Therrien: Not yet.

Ms. Laurel Collins: Did the government provide a response to why they refused to increase the funding to your office? Do you feel that the federal government is responsive to the needs of your office?

Mr. Daniel Therrien: For the extension order, there has not been a refusal. The request is still being studied.

Ms. Laurel Collins: And overall?

Mr. Daniel Therrien: Overall, I think the issue is that we're going to inherit many new responsibilities, first under this order and then under new laws in the private sector or public sector. That's why we think we need to increase our resources significantly, probably to double them. When you look at other data protection authorities, that's generally the trend.

We have had some budget increases by the government, but definitely, with new responsibilities, we will need significant new funding.

Ms. Laurel Collins: You briefly mentioned backlogs and that you had the bridge funding. Do you expect that there will be continued complaint backlogs going forward?

Mr. Daniel Therrien: At this point, we're in a situation where unless we're provided further funding, yes, we expect the backlogs to grow. But I'm an optimist, and with new laws and a new extension order, I certainly hope there will be some funding that will help ensure that we can deal with these complaints in a timely manner.

Ms. Laurel Collins: Thank you.

The Chair: Thank you.

Mr. Williams, you have up to five minutes.

Mr. Ryan Williams (Bay of Quinte, CPC): Thank you, Mr. Chair.

Mr. Therrien, thank you. I'll join the rest of the committee in thanking you for your service, sir.

You made a great statement in the text of your remarkts that it is "neither realistic nor reasonable to ask individuals to consent to all possible uses of their data in today's complex information economy", and you specifically mentioned AI. You also said, "While disruptive technologies have undeniable benefits, they must not be permitted to disrupt the duty of a democratic government to maintain its capacity to protect the fundamental rights and values of its citizens."

We're going to start with a case study just to kind of go through this. What I'd like to do is to try to relate this to changes that we need to make to Bill C-11, whenever it comes back to us. Yesterday you made a statement regarding mass surveillance of Canadians through the Tim Hortons app. Canadians who downloaded this popular app learned that their movements were being tracked every few minutes. You rightly pointed out that this kind of tracking can reveal to the company where people live, work and go to school, even where they may take medical appointments.

When it comes to Bill C-11, what changes do we need to see so that this doesn't happen further to Canadians?

Mr. Daniel Therrien: I'll speak in some detail, but I would refer you to the key recommendations for a new private sector law that accompanied a letter I sent to this committee further to its study on data mobility. There are two or three pages of specific recommendations. I'll just point to the ones most relevant to your question.

When consent is appropriate—it's not always appropriate, but when consent is appropriate—it is very important that it be meaningful. Bill C-11 would have removed from the law the requirement in the current law that consumers need to have the knowledge and understanding necessary for consent to be meaningful. I think knowledge and understanding, which was not in Bill C-11, needs to be reintroduced in the law.

Bill C-11 also allowed companies to define purposes for which they would collect information almost unfettered. Other laws provide parameters. Companies can only collect information for purposes that are "specified, explicit, and legitimate". That allows the regulator to then determine whether the purposes defined by a company were indeed specific, explicit and legitimate.

Another important factor is accountability. We think that accountability in Bill C-11 was defined to broadly. It is important that corporate accountability be defined by an objective standard, i.e., adopting procedures to comply with a law. Bill C-11 simply said that so long as companies adopt procedures, that's a demonstration of accountability. That is too subjective. The law needs to set out objective standards such as accountability means and procedures to comply with the law.

In broad terms, the law should not refer to subjective standards defined by companies or departments. The law should define objective standards that are knowable by citizens and companies. Companies would know and would have certainty through objective standards. These objective standards could be examined by the regulator to determine whether indeed the company was accountable in such a way as to comply with the law or whether there was sufficient consent based on knowledge and understanding by the consumer.

● (1630)

Mr. Ryan Williams: Thank you very much. That's very helpful before we move forward on trying to make that work for Canadians and for Canadian companies.

Just to go back to Tim Hortons right now, as a result of your intervention, did they end up stopping the tracking they were doing?

Mr. Daniel Therrien: The Tim Hortons application did indeed track their users' movements every few minutes of every day. I think that shows, among other things, that the current law—in part because it does not have penalties and in part because it does not define accountability as I've suggested—allows companies to use technology because it exists, because it may be helpful or useful, and eventually to collect information even though they may not have a direct use for it.

Before companies engage in the use of these technologies, they should be required by law to properly assess the privacy risks of that activity and they should only collect information to the extent that it is proportionate to the uses of their commercial objectives.

The Vice-Chair (Ms. Iqra Khalid (Mississauga—Erin Mills, Lib.)): Thank you.

Mr. Daniel Therrien: Frankly, I have a lot of difficulty seeing how it could be legitimate and proportional for a company, other than a telephone service provider, to follow their customers every few minutes of every day.

The Vice-Chair (Ms. Iqra Khalid): Thank you very much. That concludes your time, Mr. Williams.

I will now go to Mr. Bains for five minutes.

Go ahead, sir.

Mr. Parm Bains (Steveston—Richmond East, Lib.): Thank you, Madam Chair.

Thank you to our witnesses for joining us today.

In your submission to the Minister of Justice and Attorney General on the modernization of the Privacy Act, you indicated that you were in support of the proposed enhancement to transparency proposed in the government's discussion paper. Would explicit transparency requirements under the Privacy Act enhance the principles of open government and public trust in government institutions?

Mr. Daniel Therrien: I'm sorry. I did not catch the question.

Mr. Parm Bains: Can you hear me?

Mr. Daniel Therrien: Yes.

Mr. Parm Bains: I will repeat it.

Mr. Daniel Therrien: I heard your preamble. I did not catch the question.

Mr. Parm Bains: Would the explicit transparency requirements under the Privacy Act enhance the principles of open government and public trust in government institutions? What are your thoughts on that?

Mr. Daniel Therrien: Well, sure. Transparency and openness are well-recognized privacy principles, and it would be an improvement for the law to include them, yes.

Mr. Parm Bains: The departmental plan indicates that you anticipate legislative changes that would grant the OPC "greater enforcement powers" and are preparing the office accordingly. Have you started to make those preparations? If so, what are they?

Mr. Daniel Therrien: We're at the analysis and conceptual stage, obviously, and we're not hiring anyone because there's no legislation that has been adopted, but again, I thought it would be important not to be caught off guard and to think internally how we would we organize and what kinds of professionals we would we need to exercise this or that new responsibility, including adjudication, so that if a new legislation contains similar provisions as Bill C-11, we would have a head start and might be able to hire people, develop procedures and develop policies.

One area where we intend to do some work is again on this question of order-making and adjudication. That activity will most likely require rules of practice, which will have an impact on the regulated entities, who obviously will want us to act fairly in adjudicating complaints. We have started to give some thought to what would be the adjudication process so that we can consult stakeholders as to whether we have it remotely right, and that would accelerate the adoption of these rules.

● (1635)

Mr. Parm Bains: Thank you.

What progress did you make on paving the way for increased informed consent and what are your hopes for the new commissioner in this respect?

Mr. Daniel Therrien: What would be my recommendations for enhanced consent?

Mr. Parm Bains: Yes, informed consent.

Mr. Daniel Therrien: If we're talking about the private sector, I would refer you again to the two-page key recommendations, including primarily reintroducing in the law the requirement that consent requires the consumer to have knowledge and understanding of the purposes for which the information is about to be used. That requirement was omitted from Bill C-11, and I think that's an important problem. It would not lead to meaningful consent.

Mr. Parm Bains: How much time do I have, Madam Chair?

The Vice-Chair (Ms. Iqra Khalid): You have about a minute left.

Mr. Parm Bains: We had the Information Commissioner at the committee. In response to being asked about the effects of remote work on her office, she said that she was very pleased and surprised that the office was able to close a record-breaking 6,800 cases last year. What has been the OPC's experience with remote work? Have you had the same success as the Information Commissioner's office?

Mr. Daniel Therrien: Remote work is effective. Very early, after the onset of the pandemic in March 2020, we moved to a teleworking arrangement, and the vast majority of our people work remotely and effectively. This coincided for us, though, with the sunsetting of a special budget that we had to tackle a backlog of complaints. We had almost eliminated our backlog. It's starting to increase slightly, but we're still in a good position overall.

The Vice-Chair (Ms. Iqra Khalid): Thank you very much.

Thank you, Mr. Bains.

[*Translation*]

Could you please begin, Mr. Lemire?

Mr. Sébastien Lemire: Thank you, Madam Chair.

Thank you also for making an effort to speak French.

Mr. Therrien, in the winter and spring of 2022, the Standing Committee on Access to Information, Privacy and Ethics conducted a study on the collection of use of mobility data by the federal government. Further to your written replies to questions from committee members and the resulting report, how urgent is it for Parliament to audit or conduct a legislative review of federal privacy legislation?

Let us consider PIPEDA specifically. We know that Minister Champagne was supposed to introduce reforms this winter.

Mr. Daniel Therrien: It is urgent, to say the least, and should have been done some time ago. I think the government knows there is a problem with trust in the digital economy. That is why Bill C-11 was introduced at the time. We had certain concerns about the content of the bill.

As to the private sector, the act is 40 years old, and 20 years old for the private sector, preceding the creation of Facebook by five years. The world has completely changed since these laws were passed and there is obviously an urgent need to update them.

● (1640)

Mr. Sébastien Lemire: This is fascinating, indeed.

Mr. Therrien, are there times during your tenure when you have witnessed actions the government has taken, or even a lack of action, that impacted the privacy of Canadians?

Have you witnessed times when political interest was prioritized over the common good?

Mr. Daniel Therrien: The fact that we do not have laws adapted to the technologies of the fourth industrial revolution at the beginning of the 21st century creates in itself an environment that gives rise not only to potential risks, as I said, but to real harm for individuals.

Would the Tim Hortons app situation still have occurred if the laws had been modernized? Maybe, but the chances would have been much less. Would the Clearview AI problem have occurred if the laws had been adapted to modern technology? Again, the chances would have been much lower. Regulation will not solve everything, but a strong law, rigorously enforced, and sometimes with penalties, is an incentive for all actors, departments and companies to respect the law. Clearly, Canada's delay in adopting modern laws has resulted in situations that have caused harm to Canadians.

Mr. Sébastien Lemire: There is certainly a danger in inaction.

The Vice-Chair (Ms. Iqra Khalid): Thank you, Mr. Lemire.

[*English*]

We'll now go to Ms. Collins for two and a half minutes.

Please go ahead.

Ms. Laurel Collins: Thank you, Madam Chair.

According to the departmental results indicator listed in the departmental plan, in the most recent fiscal year, only 45% of Canadians felt that businesses were respecting their privacy rights.

From your perspective, why is this number so low? The target for this indicator is 90%. What measures need to be taken to achieve that goal? Also, do you think that goal is achievable by the deadline of March 2023?

Mr. Daniel Therrien: By March 2023, probably not.

Is it a realistic target to say that 90% of Canadians should have confidence that their data is appropriately protected by companies and government? I think it is. How long that should take—

Ms. Laurel Collins: What measures need to be taken in order to reach that target?

Mr. Daniel Therrien: I think it's a function of a series of measures. It starts with a law that actually protects the privacy of citizens and consumers. It starts with that. As I say, it also requires that the regulator have appropriate resources, and I've said that I think we need to double our complement to apply the new laws that are about to come. The laws need to provide incentives for companies and departments to comply with the law. That is, in big part, what is missing currently.

Technologies do exist. They are attractive and—

Ms. Laurel Collins: I'm sorry to interrupt, but we have such limited time.

You also mentioned the need for independent, proactive audits. You mentioned it in your comments and in your introduction.

Can you talk a little bit more about why this is so necessary and how it would actually improve the work of your office?

Mr. Daniel Therrien: In short, because individuals are not in a position to understand and know how their information is collected and used given today's technologies, there needs to be an independent third party like the OPC who can actually look under the hood, as we say, and do proactive audits to bring the level of confidence up because we cannot rely only on consumers to identify issues that they complain about.

The Vice-Chair (Ms. Iqra Khalid): Thank you very much, Ms. Collins.

We'll now go to Mr. Bezan for five minutes.

Go ahead, sir.

Mr. James Bezan (Selkirk—Interlake—Eastman, CPC): Thank you, Madam Chair.

I congratulate and thank Commissioner Therrien for his very successful career, his service to Parliament and his service to all Canadians in the important work that his office has conducted over his tenure.

You said in your opening comments, Commissioner, that there could be no innovation without trust and there's no trust without the protection of rights. You're talking about industry and industry stakeholders. You go on to say that interoperable laws are in Canada's interest.

As we move forward as legislators, as you quite eloquently said, it's our responsibility at this committee, in the House of Commons and the Senate, to develop these new laws. What is the gold standard that we should be looking at for interoperability with other countries to ensure that our businesses and industries are competitive, while protecting the privacy rights of all Canadians?

● (1645)

Mr. Daniel Therrien: I hesitate to talk about the gold standard. Many people, when asked what the gold standard is, refer to the European Union's GDPR. It is certainly an excellent standard. There are similarities between our recommendations for law reform and the European GDPR. It is an excellent standard. Other countries have adopted similar laws—not exactly the same law.

I'm not advocating that Canada adopt a carbon copy of the GDPR, but there are elements of the GDPR that make a lot of sense, such as the rights basis, proactive audits and objective standards. By the way, the GDPR is sometimes, if not often, characterized as “prescriptive”, i.e., adopting rules that are too minute and get in the way of commercial operations. This is in contrast to Canada's laws, which are principles-based—PIPEDA being principles-based.

I think it is a misconception to talk of the rights-based law as a prescriptive law. A principles-based law is in Canada's interest. We need to have tech-neutral and industry-neutral laws in the technological sector. That makes a lot of sense. In the very same way, a rights-based law protects citizens with rules that are at the same level of generality as a principles-based law. Therefore, both principles-based law and rights-based law are equally adaptable and flexible to the digital world, which is a necessity with the digital world.

Mr. James Bezan: We have the digital world that we have to work in, and then you also have the standpoint of working within confederation. As we know, every province is ultimately responsible for the regulation of the majority of businesses and industries, including on the privacy side, as we just saw with the investigation that you did of Tim Hortons' app with the privacy commissioners of other provinces

Are there any laws coming down at the provincial level that we should also be looking at adapting, or should the federal government be leading and the provinces be adapting to the laws that we bring in? As you said, they should be principles-based to ensure that we continue to have innovation and aren't creating too much red tape that will hamstring our businesses here.

Mr. Daniel Therrien: At this point, the most modern law is the Quebec law, which is also a rights-based law. Some say that it is too prescriptive in some regards, for instance, in how it deals with cross-border data transfers. It may be a legitimate criticism of that law, but there are many elements of the recent Quebec law that I think you should be considering.

I would say that Ontario, of course, has not adopted a new law, but has put out very detailed and thoughtful consultation papers on how it might regulate the private sector. That is also worthwhile. British Columbia had a parliamentary committee that issued a report along those lines. All three of these provincial jurisdictions are advocating for rights-based laws.

Mr. James Bezan: I appreciate that.

A final question I have—and I believe I am probably getting close to the end of my time, Madam Chair—is on the investigation of Tim Hortons that you did. Quickly, how can you make sure that all of the data they collected has been purged permanently from their databases?

Also, are you aware of any other investigations being conducted against other companies that have apps that track the mobility data of Canadians?

The Vice-Chair (Ms. Iqra Khalid): That concludes your time, Mr. Bezan, but I'll ask Monsieur Therrien if he wants to answer briefly.

● (1650)

Mr. Daniel Therrien: We have a commitment from Tim Hortons that they'll delete it. If we have reason to doubt that, we can ensure that through technological means.

At this point, no, there is no other investigation under our control on geolocation. We hope that the lessons of Tim Hortons will apply to other companies.

Mr. James Bezan: Thank you.

The Vice-Chair (Ms. Iqra Khalid): Thank you very much.

We'll now go to Ms. Saks for five minutes.

Go ahead, Ms. Saks.

Ms. Ya'ara Saks: Thank you, Madam Chair

Thank you, Monsieur Therrien.

Monsieur Therrien, in our conversations with you in this room, we have talked about the notion of de-identified data in relation to PHAC. I have a few questions I want to ask in the time that we have, but could you just briefly provide an update on the investigation you conducted on the de-identified data in relation to PHAC?

Mr. Daniel Therrien: It's still ongoing.

Ms. Ya'ara Saks: Okay, so there's no conclusion as of yet from it?

Mr. Daniel Therrien: No.

Ms. Ya'ara Saks: That takes me into more of a general question of where we're at. Given that you expressed your support for innovation, but being mindful of its applicability in terms of privacy, and given that mobility data can improve everything from how we manage our public health to where businesses put their shops—and Google knows where I and all of us go grocery shopping weekly—and the associated privacy protections that are needed to support innovation, do you support establishing a standard for the de-identification of data? We heard here, for example, of privacy by design. Do you support a set of standards for that?

Mr. Daniel Therrien: Yes, with the condition that technology will change. A standard that would be a good standard in 2022 might no longer be good in 2028. This would need to be reassessed with technology. There might be a technology that makes re-identification in 2028 much easier, for instance, so the standard would need to evolve. But, yes, the idea of having a standard is certainly appropriate.

Ms. Ya'ara Saks: I'm going to switch gears a little bit.

In the day and age we're in, I have an intern here from Ukraine as part of the parliamentary internship program. She showed me on her phone that she has a digital passport with her code passport and her essential documents, including her birth certificate and other important pieces of ID that she's able to access, which is very helpful for her, considering that she's coming from a war-torn country and that documents may get lost and so on.

There's a lot of interest in the concept of digital IDs and having access to them. Could you explain how such a technology could potentially strengthen privacy security? Canadians have questions about how all that could potentially work.

Mr. Daniel Therrien: Digital ID, like all technologies, can be helpful and privacy protective or harmful to privacy depending on how it is designed. It is certainly conceivable that digital ID could enhance the verification process and the authentication process, allowing citizens to have access to services.

It is certainly conceivable that digital ID would be better from a privacy perspective than SIN numbers and the antiquated ways we have to identify ourselves currently. It all depends on how the technology would be designed. It is certainly possible that digital ID would lead to the data being available to many players or actors, corporate or governmental, that should not have access to all of this data, but it doesn't have to be designed that way. It could be designed in a way that provides authentication, which is the first part, and then controls correctly who in a department or who in a company has access to what information because they have a legitimate need for it.

Ms. Ya'ara Saks: Thank you for that.

In the Canadian context we're in—and obviously there's also an issue with jurisdiction—some of our identification like driver's licences and OHIP cards—I'm from Ontario—are under provincial jurisdiction, but at the same time, we have social insurance numbers and passport numbers at the federal level. Do you think it's time for us as parliamentarians to take a deep dive into how we can best serve Canadians but also protect their privacy and enable them to move through this digital space with ease as well as with safety and security?

● (1655)

Mr. Daniel Therrien: Yes. I think digital ID is certainly an issue that has the potential to enhance access to services in a privacy-protected way. It's important to design it properly. It's entirely an issue worthy of consideration.

Ms. Ya'ara Saks: Have you encountered international best practices in other countries? I gave Ukraine as an example, but has that come across your desk?

Mr. Daniel Therrien: Estonia is often referred to, but it is a very small country with a very small population. It is a model, and if need be, my office could provide other examples, if you wish.

Ms. Ya'ara Saks: I would love some kind of written outline of best practices internationally. Thank you.

Mr. Daniel Therrien: Sure.

Ms. Ya'ara Saks: I think I'm out of time. Thank you.

The Vice-Chair (Ms. Iqra Khalid): Thank you very much, Ms. Saks.

Thank you, Monsieur Therrien.

I put this to members. We have a couple of minutes before we have to go in camera for committee business. If there are any brief questions that members want to ask, let me know.

Mr. Damien Kurek: I have one question, if I may.

The Vice-Chair (Ms. Iqra Khalid): Okay, so we'll just follow the same order. I'll come to you, and then I'll go to the Liberal side, the Bloc and then the NDP.

Go ahead, Mr. Kurek.

Mr. Damien Kurek: Sure. Thank you.

Thank you, Commissioner. I hope this was a good way to end your distinguished service with us.

You mentioned StatsCan in your opening remarks. I want to give you an opportunity to elaborate a little bit more about some of the concerns you have regarding financial information and some of the details of Canadians that Stats Canada would possibly have been able to get.

Mr. Daniel Therrien: Statistics Canada is a good example leading to my answer to Ms. Saks, namely that the principal amendment to make to the public sector law is to have a standard of necessity and proportionality limiting the collection of information by government institutions.

Statistics Canada had laudable objectives of better understanding certain problems of the poor's access to programs, so it went about getting extremely detailed—actually line-by-line—financial reports of banks and financial institutions to better understand citizens in order to give them access to better services. In our view, this very pervasive look at financial records was not proportional and necessary. We did not say that the objective was not laudable and legitimate, but there was just too much information obtained by this government institution. We have since worked with Statistics Canada and are still working with them to improve their systems, but I think the main lesson is that it is crucial that the standard of necessary proportionality be incorporated in a future public sector law.

The Vice-Chair (Ms. Iqra Khalid): Thank you very much, Mr. Kurek.

If the committee doesn't mind, I'll ask a very brief question from the chair.

Monsieur Therrien, given your experience through all of this, are there any recommendations you would make to a future privacy commissioner as to how to work better with government and how to really address the issues of how digital governance and technology really impact privacy for Canadians? Also, is there any advice you would give to Canadians with respect to how they can proactively protect their own privacy in that digital space?

Mr. Daniel Therrien: I've actually started a number of activities during my term for the OPC to not only investigate violations after the fact but also to give advice to companies and departments as they design programs to ensure that those programs comply with the law.

We've already started quite a few engagement activities with government departments, and they are more and more popular among government departments. I would encourage the new commissioner to continue on that path. It is unquestionably much better to think about privacy protection—it's the privacy by design concept—early in the development of a program or initiative than at the end, obviously. We have started discussions, and we would encourage further discussions.

By the way, these discussions will hopefully provide better knowledge of privacy principles on the government side. On our side, it provides a better grounding of operational realities within which our privacy principles are to be implemented. It's a good and useful two-way conversation to have. I'm not saying it's always that meaningful and useful, but that could be one improvement to be made. We should continue these engagements to ensure that there's a true dialogue between the regulated entities that engage with us, and to be really conscious and aware of the context within which departments operate.

For Canadians, “Stay alert.” My overall thought is that given the complexity of new technologies and business models, I'm not expecting people to read 50-page privacy polices to protect their privacy. That's why a regulator is not a panacea, but it is really fundamental and essential. It will not solve the problem by itself, but it is really important that citizens have an expert body like the OPC to look after them, have their backs, and protect them.

Yes, there are certain measures that can be taken, but there is a very important limit nowadays to how people can actually protect their privacy.

● (1700)

The Vice-Chair (Ms. Iqra Khalid): Thank you very much.

Next, we have Monsieur Lemire.

[*Translation*]

Mr. Sébastien Lemire: Thank you, Madam Chair.

Mr. Therrien, I hope you will remain active and continue to serve the public interest, perhaps as a professor, who knows? I would like to see what happens next.

In closing, I would like to hear from you about the integrity that your mandate as Privacy Commissioner requires. I would therefore like to ask you the following question very directly.

What would you like to add today to everything that has already been said?

Mr. Daniel Therrien: I think the level of understanding and knowledge about the issue of privacy among the population is better now than it was eight years ago. That's one of the things I'm quite proud of. I don't claim that people are experts in privacy, far from it, but privacy used to be seen as an issue for experts, for technologists or for people who are maybe not quite on earth. Now we see that privacy is connected to the exercise of fundamental rights: democracy, in the case of Cambridge Analytica, surveillance, in the case of Clearview AI and Tim Hortons, etc.

Privacy is important, and I think people understand it better. It's a bit confusing, but people have a better understanding. It may bring some behavioural changes in the population. I hope it will especially lead to people putting more pressure on elected officials to pass the laws needed to protect them.

I don't think any consumer is asking for the right to have more privacy policies to read in order to be able to give consent. I believe that citizens want to participate in the digital economy and receive digital services from government in a secure manner, knowing that laws have been passed to protect them and that public bodies have been appointed to ensure that their rights are respected.

Mr. Sébastien Lemire: This is not trivial.

Thank you very much.

[*English*]

The Vice-Chair (Ms. Iqra Khalid): Thank you very much.

Last, but not least, we'll have Ms. Collins. Please go ahead.

Ms. Laurel Collins: Thank you again.

Reflecting on your past eight years, what do you see as the biggest challenge you faced, and what advice would you give to members of Parliament to support the next privacy commissioner?

Mr. Daniel Therrien: I think the biggest challenge is the appeal of new technologies. They can be very helpful and useful to society and to companies. Some companies have become extremely profitable. They provide very helpful services, but because new technologies are appealing and cheap to use, we forget that they also create harms. It is essential that the laws and how they are applied continue to facilitate responsible innovation, but reintroduce the idea that it should not be the wild west, that the Internet is not an unregulated place. It needs to be properly regulated, but it needs to be regulated in a way where, again, the rights we have acquired over the years, if not centuries, like privacy, are not set aside because technology is so easy, appealing and profitable.

● (1705)

The Vice-Chair (Ms. Iqra Khalid): Thank you very much.

I'll take the opportunity now to thank you, Monsieur Therrien, for his service and for coming here today to answer our questions. On behalf of this committee, we wish you all the very best.

Mr. Williams, I see that you have your hand raised.

Mr. Ryan Williams: Madam Chair, I just have one quick question, if you would allow me, as we have Mr. Therrien here for the last time.

The Vice-Chair (Ms. Iqra Khalid): If you ask your question in 30 seconds or less, we'll allow Monsieur Therrien to answer briefly. Please go ahead.

Mr. Ryan Williams: Thank you so much.

Mr. Therrien, I want to ask about exceptions for consent. Bill C-11 mentioned some exceptions for consent, and you mentioned telecommunication carriers. What other examples have you seen for exemptions for those looking for consent from Bill C-11?

Mr. Daniel Therrien: Our submission on Bill C-11 dealt with that in detail.

I would say that one case that comes to mind would be research, for instance. Health was mentioned earlier in this conversation. Research for health purposes could be, within certain parameters, an exception to consent. Bill C-11 had exceptions to consent that were way too broad, but as I said, consent is not a panacea. It is normal that there would be some exceptions to consent.

The Vice-Chair (Ms. Iqra Khalid): Thank you very much.

Mr. Ryan Williams: Thank you, sir.

Thank you very much, Madam Chair. I appreciate it.

The Vice-Chair (Ms. Iqra Khalid): Thank you again, Monsieur Therrien.

We are now going to suspend for about five minutes as we go in camera for committee business.

[*Proceedings continue in camera*]