HOUSE OF COMMONS
CHAMBRE DES COMMUNES
CANADA

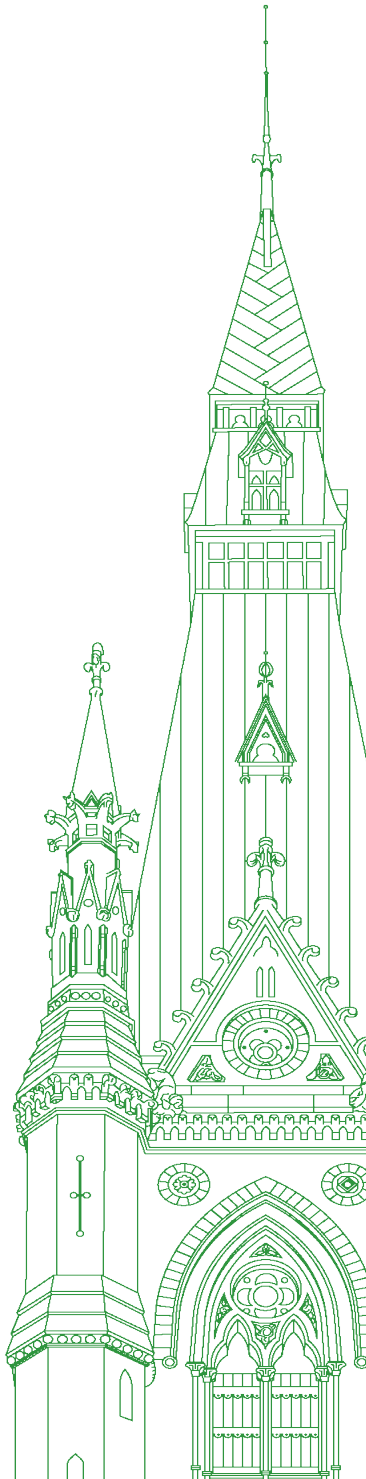
43rd PARLIAMENT, 2nd SESSION

Standing Committee on Access to Information, Privacy and Ethics

EVIDENCE

NUMBER 034

Monday, May 10, 2021



Chair: Mr. Chris Warkentin

Standing Committee on Access to Information, Privacy and Ethics

Monday, May 10, 2021

● (1100)

[*English*]

The Chair (Mr. Chris Warkentin (Grande Prairie—Mackenzie, CPC)): I call this meeting to order.

This is meeting number 34 of the House of Commons Standing Committee on Access to Information, Privacy and Ethics. I'd like to remind committee members and those who have joined us that today's meeting will be televised and will be made available on the House of Commons website.

For the first hour of our meeting today, pursuant to Standing Order 81(4), we are examining the main estimates 2021-22, votes 1 and 5 under the offices of the Information Commissioner and the Privacy Commissioner of Canada.

Today, some witnesses for the first hour will be joining us for the second hour. They will remain here for the second hour for what is technically our second meeting today. For our first hour, from the Office of the Privacy Commissioner of Canada, we have Daniel Therrien, who is the Privacy Commissioner of Canada; Brent Homan, who is the deputy commissioner of the compliance sector; Daniel Nadeau, who is the deputy commissioner of the corporate management sector; and Gregory Smolynec, who is the deputy commissioner of the policy and promotion sector. He wasn't here moments ago but may have joined us. If he hasn't yet, he will be joining us.

Commissioner, I'll turn it over to you for your opening statement.

Mr. Daniel Therrien (Privacy Commissioner of Canada, Office of the Privacy Commissioner of Canada): Thank you, Mr. Chair. Can you hear me?

The Chair: I can, very well. Thank you.

[*Translation*]

Mr. Daniel Therrien: Good morning, Mr. Chair and members of the committee.

I am pleased to meet with you for the next two hours to discuss our 2021–22 Main Estimates, our activities in general, and then the fundamental issue of facial recognition. All of this, of course, in a context where a very important bill, Bill C-11, has been introduced in the House of Commons.

Last year was one of transition for many organizations, and our office was no exception. We quickly shifted to adapting our processes to continue serving Canadians during the pandemic.

It was also a year of transition on the budgetary and legislative fronts. Our office received a permanent increase of 15% in the 2019 federal budget to address the most urgent needs of the OPC pending legislative reform. This allowed our office to expand our policy and guidance functions, to enhance our advisory services for organizations and to address pressures resulting from new mandatory breach reporting requirements in the private sector.

We also received temporary funding to help us reduce a very large part of our investigative backlog of complaints older than a year. We met and even surpassed our target and reduced the overall backlog of complaints by 91%. We are very proud of that.

Over the past year, our work has included the publication of guidance on protecting privacy during a pandemic, as well as a contextual framework for government institutions to protect privacy in the context of COVID-19 initiatives. Consistent with this framework, we reviewed and advised the government on the COVID Alert app. Following a public consultation, we released key recommendations for regulating artificial intelligence.

We also completed our first breach records inspections report—again, this is about data leaks. In addition, we analyzed and provided recommendations on several legislative initiatives. This included a submission on the statutory review of the Access to Information Act, another submission on the modernization of the public sector Privacy Act, which was the subject of a consultation by the Department of Justice.

Finally, after a detailed analysis of Bill C-11, we completed another brief. All these documents, with the exception of our brief on Bill C-11, are available on our website.

While the injection of funds in the 2019 budget helped us to reduce our backlog and to increase our capacity, there is still a very significant gap. Given the marked acceleration of digitization caused by the pandemic, we continue to struggle meeting the demand in guidance, guidelines and advisory work, and to assist our investigators to address complaints filed by concerned Canadians.

In the government's fall economic update, funds were allocated to support the implementation and enforcement of Bill C-11. This is clearly a good thing. However, now that we know the extent of our new responsibilities under this legislation, we believe additional funding will be required.

● (1105)

[*English*]

Bill C-11 imposes several new responsibilities on the OPC, including the obligation to review codes of practice and certification programs and give advice to individual organizations on their privacy management programs. It should be noted that these are non-discretionary activities, meaning that every time an entity or organization seeks our advice or approval, we will be required to provide our considered opinion.

We welcome the opportunity to work with business. In recent years, I have restructured my office towards a greater proactive approach to guide and engage with organizations toward compliance with the law. We created two new directorates to engage proactively with private and public sector organizations, on a voluntary basis, on privacy risks of a high-impact nature. These activities have increased during the pandemic. Actually, they've been very popular.

As you know, another role we play is to investigate complaints alleging violations of the act. However, it is not our only role. In order to be an effective regulator, we must be able to be strategic in our enforcement and advisory activities, applying a risk-based approach.

As we explain more fully in our submission on Bill C-11, we are concerned that with the non-discretionary nature of our responsibilities under that bill, we will not be able to both serve complainants and organizations and focus on harms to Canadians in general. The issue here is not primarily financial, although in our view additional resources will be required. The OPC should have the legal discretion to manage its caseload, respond to the requests of organizations and complaints of consumers in the most effective and efficient way possible, and reserve a portion of our time for activities we initiate, based on our assessment of risks for Canadians. Such discretion is enjoyed broadly by domestic and international regulatory partners, both within and outside the privacy protection sphere.

Another option to balance our various activities could be ensuring that the OPC's role of approving codes of practice and certification programs under the proposed Bill C-11 be conditional on the payment of a cost recovery fee to ensure that we have the capacity for that task as well as for our other priorities. No regulator, ultimately, has enough resources to handle all the requests it receives from citizens and regulated entities. It is important that my office have the flexibility to allocate resources in ways that will offer the most benefits for Canadians and adjust activities to address new and emerging trends.

In addition to changes brought by C-11, proposals made by the Department of Justice in its recent consultation on modernizing the Privacy Act, the public sector act, would also see significant changes to our role in the public sector, of which we are largely supportive. This includes a new public education mandate, the power to issue guidance to government institutions, a role in issuing advance opinions and overseeing pilot projects, and greater discretion to publish compliance outcomes, among others. Justice's proposals also include an enhanced compliance role for our office, such as expanded proactive audit powers and a form of order-making. We have already begun to plan for these eventualities.

● (1110)

[*Translation*]

In closing, I would like to point out the fact that, as we look to the future, it will be important that modern privacy laws allow us to act as an effective regulator. Our office should also be provided with the financial resources necessary to implement these laws.

I look forward to working with Parliament on improving the legislative proposals to ensure our modern privacy laws adequately protect the privacy rights of Canadians, while promoting responsible innovation.

Thank you for your attention.

I welcome your questions.

[*English*]

The Chair: Thank you, Commissioner.

Dr. Carrie, we'll begin our first questions with you.

Mr. Colin Carrie (Oshawa, CPC): Thank you very much, Mr. Chair.

To our witnesses, I really want to thank you for being here today. I've been looking forward to having you here.

As you mentioned, this is an unprecedented time. We are seeing more and more people working from home. I'm wondering if you were able to identify any efficiencies in program delivery by having people work at home. Are you finding that things are working okay right now, or do you have something to suggest?

Mr. Daniel Therrien: We have efficiencies, but not really due to the telework environment. We had to adjust very rapidly, obviously, to the telework environment, ensuring that our colleagues, our employees, had the required technology to continue to provide their services. There was no increased efficiency due to the pandemic, but there was no loss of efficiency either.

There were efficiencies due to technology regardless of the pandemic, in that, for instance, we used, for the first time, an electronic form for the filing of complaints leading to investigations. That allowed us to be more efficient in the first stages—the triage part of our investigations. So technology did help at the end of the day, yes.

Mr. Colin Carrie: Long-term, do you see a significant impact on your resources? Do you think, long-term, that it will allow you to run things more efficiently?

Mr. Daniel Therrien: Technology will certainly be part of the solution. We're working right now on a way to use technology when we receive breach reports, for instance, by companies. We think that automation can help increase efficiency in reviewing these reports.

At the end of the day, though, I think the greater use and the huge acceleration of technology in recent years, and particularly due to the pandemic, means that we have many more issues to examine. Overall, there's a need to increase resources, but we're doing what we can to increase efficiencies.

● (1115)

Mr. Colin Carrie: I think we live in a very exciting time, in many ways, but the questions I get at my office about personal privacy and data collection seem to become more and more important as time goes on.

You mentioned there was an increase of 15% with the budget this year and that you are preparing for legislative changes. You mentioned Bill C-11.

One of your comments I found a little bit curious. You mentioned that you make your briefs available on the website, but you mentioned that the brief on Bill C-11 was not on the website. Was there any issue? Why is it not on the website?

Mr. Daniel Therrien: It's simply due to the fact that I have not yet been called to testify on Bill C-11. I'm waiting for members of Parliament to send me an invitation. We're ready to go, and as soon as we have a request from members of Parliament, we will be very glad to oblige and put this up on our website.

Mr. Colin Carrie: Excellent. That's very good.

I'm hearing more and more from people that this field, especially in digital media, is innovating so quickly that there is difficulty for regulators to keep up.

You mentioned that because of things moving so quickly, and new legislation, you could foresee the requirement for more resources in your office. Do you have any thoughts on how much that might include for the taxpayer?

Mr. Daniel Therrien: As I mentioned in my statement.... First of all, I need to acknowledge that in the economic statement of last fall, I believe something in the order of $18 million annually was set aside in that quasi-budgetary document. However, this was not only for the OPC, but for all of the government institutions that will be called upon to implement Bill C-11. We will have a share of it.

That amount was arrived at after consultation with our office before we saw Bill C-11. Now that we see Bill C-11, we see, in particular, our role in approving codes of practice by industry and giving advice upon request to companies about their privacy programs. We did not know that when we gave our estimates to the government, but now that we do, increased funding will be required.

Beyond increased funding—and I'll repeat the point that I made in my statement—we are totally welcoming of the role given to us by Bill C-11 on codes and advice to companies. However, frankly, we cannot do that for each and every request that we will receive. It's why I think we want to engage with business in that regard. Some additional funds will be required, but we also need discretion to manage our workload and to continue what we have done until now, which is to offer our services but not have to answer each and every request. We deal with those that seem to raise the higher privacy risks, for instance.

This is in part about money and in part about discretion for us to say yes to most requests but no to others if our budget cannot accommodate this.

The Chair: Thank you, Mr. Carrie.

We'll turn to Mr. Fergus now for the next questions.

Mr. Fergus, go ahead.

[*Translation*]

Mr. Greg Fergus (Hull—Aylmer, Lib.): Thank you very much, Mr. Chair.

I'd like to thank Mr. Therrien for his speech and for appearing before the committee today.

Mr. Therrien, I found your remarks very interesting.

My first question is very simple, but it will lead to other questions.

Has the pandemic had a significant impact on your office's resources?

● (1120)

Mr. Daniel Therrien: In a word, yes.

Mr. Greg Fergus: Can you elaborate on that?

Mr. Daniel Therrien: Before the pandemic, we were already in a world where a digital revolution was unfolding. The pandemic made this revolution explode. As a result, public and private organizations, including commercial enterprises, are having to go increasingly digital and are therefore asking us more questions about how to do things in a privacy-friendly way.

A number of businesses and organizations have come to us, including a group in Toronto that provides advice to businesses across Canada, as well as a number of federal government departments, particularly Health Canada. These groups have turned to us for advice on new programs that have had to be created extremely quickly as a result of the pandemic to ensure that this is done in a way that respects privacy.

Mr. Greg Fergus: This leads me to my second question.

When I read the office's departmental plan, I see that you continue to take initiatives to investigate and review situations that have significant privacy implications, such as those that affect an entire sector or industry. You have said that you will continue to do so as long as resources allow.

How do resources limit your office's ability to conduct investigations on its own initiative?

Mr. Daniel Therrien: There is no shortage of topics that could be investigated. So we need to use our resources to investigate the topics that pose the most risk. For example, we started an investigation into the use of artificial intelligence in employment. This seemed to me to be a particularly important issue because of the serious risks it poses for job applicants.

The challenges lead us to make choices. For all departments, financial resources are not unlimited, and we are not asking for an unlimited budget either. It's normal that our financial capacities have limits. We try to allocate our activities based on a risk analysis. Among our activities are investigations, which we take the initiative on, as opposed to complaints. People come to us with complaints that we have to respond to. It's important to respond to them because, for them, we are a mechanism for access to justice for citizens. However, they will not necessarily be aware of the practices that are the most risky for privacy, hence the need to be able to start investigations ourselves. We need to be able to do both.

Furthermore, we also need to play a proactive role, for example, by providing advice to companies and government departments and issuing guidelines. Bill C-11 will give us an approval role in codes of practice and allow us to advise companies. All of this is great, but because of the accelerating digital revolution, we need more funding. We are in the process of quantitatively assessing our needs. Unfortunately, some requests will have to be denied because we can't do everything.

Mr. Greg Fergus: I have less than a minute left. I'm going to ask you a simple question, but one that you may have difficulty answering.

How much do you think your budget should be increased to allow you to do your job reasonably over the next three years?

● (1125)

Mr. Daniel Therrien: I'll go out on a limb and say that in terms of the private sector, it's probably about 50%. In addition to that, new roles would be given to us as part of the Department of Justice's proposed reform of the public sector, if that were to happen in the not-too-distant future. A substantial increase in the budget would then be required.

Obviously, Parliament will make a decision based on the scope of our requests. However, we're talking about a substantial increase because of two factors: the acceleration of the digital revolution and the privacy issues this poses, on the one hand, and on the other, the new responsibilities we'd have under this bill.

Mr. Greg Fergus: Thank you very much, Mr. Therrien.

[*English*]

The Chair: Thank you, Mr. Fergus.

We're going to turn to Mr. Fortin.

[*Translation*]

Mr. Rhéal Fortin (Rivière-du-Nord, BQ): Thank you, Mr. Chair.

Good morning, Mr. Therrien.

I just heard you answer questions from my colleague Mr. Fergus. Some of the answers surprised me, and I wonder if we should be concerned. To the last question, you responded that the budget increase needed to meet your obligations in the private sector would be in the order of 50%.

So you would need 50% more money to be able to fulfill your mandate. Do I have that right?

Mr. Daniel Therrien: Actually, that money would be needed because of the additional mandate we would have under Bill C-11.

Mr. Rhéal Fortin: Leaving aside Bill C-11, as it stands now, would you say that you have the budget to carry out your mandate, apart from what may happen next with Bill C-11?

Mr. Daniel Therrien: The digital revolution, which requires us to provide more advice and set more guidelines, is always a factor. For example, we give guidelines to companies. These are guides, which are not legally binding. A few years ago, after a consultation, we identified about 30 topics for the private sector that should be covered by privacy guidelines. We're not even halfway there.

Although we have budgets, and they have been increased, if we look at our overall activities, we find that we have been unable to update guidelines for businesses and support for individuals because the digital world raises too many new issues. We're unable to provide the amount of advice, the amount of guidance, that we should be able to provide.

Mr. Rhéal Fortin: Obviously, as you've already said, the pandemic situation isn't helping. The increase in communications on social media, meetings—like this one this morning—that are held through the Zoom platform, but that we would normally attend in person on the Hill, must be major challenges for the Office of the Privacy Commissioner.

Could you tell us about the kinds of challenges you face in the context of the pandemic?

Mr. Daniel Therrien: This takes many forms. As I was telling Mr. Fergus, many companies, departments and government entities are seeking our advice on pandemic-related initiatives. It's also important to be aware of how the technology is being used in a pandemic context. I have mentioned before that technology is being used much more in these circumstances for service delivery, particularly in education and health care.

How can this be done in a way that respects the privacy of information shared on digital platforms? We're looking at that. There are investigations. We note things that need to be investigated. I gave you an example earlier of the use of artificial intelligence in job interviews. We'll also talk about facial recognition later.

So we try to use our budgets as best we can, based on the risk we see.

● (1130)

Mr. Rhéal Fortin: Right now, you don't necessarily have all the funds you need to carry out your mission, but have you established any kind of guidelines or criteria for what you will say no to?

For example, you told us earlier that you had received requests to update directives, but that you were only able to do part of the work. How do you prioritize? How do you decide what you're going to do and what you're going to set aside?

Mr. Daniel Therrien: Our assessment of risk based on what we observe in various settings is what determines it. In this context, the current and future legislation, as part of Bill C-11, requires us to investigate when complaints are referred to us.

Except in very rare cases, when a complaint is filed by an individual, the legislation requires us to investigate. This is a real constraint. Again, there are advantages to this system, particularly in terms of access to justice. We're an ombudsman with a relatively expedited process, one that is simpler than judicial tribunals.

I understand all of that, but the fact remains that it creates a real constraint because we have to investigate every complaint that comes in. We believe that, like other privacy regulators, we should have more flexibility. The question is what recourse there would be if the office were unable to investigate a complaint. One of the things Bill C-11 talks about is a private right of action before the courts.

These are sensitive issues, but having to investigate every complaint we receive is a real constraint.

Mr. Rhéal Fortin: As I understand it, you can do less prevention. Can we say that the lack of funding is having a negative effect on prevention?

Mr. Daniel Therrien: Basically, yes.

Mr. Rhéal Fortin: Thank you, Mr. Therrien.

[*English*]

The Chair: Mr. Fortin, your time is up, unfortunately.

We're going to turn to Mr. Angus now for the next questions.

Mr. Charlie Angus (Timmins—James Bay, NDP): Thank you, Mr. Therrien. It's a pleasure to have you back before our committee.

As you know, we have been studying the issue of non-consent videos and photos of people being on the site Pornhub MindGeek. Are you presently involved in an investigation of whether or not they have breached the privacy rights of Canadian citizens?

Mr. Daniel Therrien: Yes.

Mr. Charlie Angus: Okay. You have undertaken an investigation, then.

Mr. Daniel Therrien: Yes.

Mr. Charlie Angus: I imagine you're not able to tell us anything about your investigation.

Mr. Daniel Therrien: That's correct.

Mr. Charlie Angus: I fully understand.

I'm interested because one of the survivors who approached us had tried to get the RCMP to investigate. The RCMP are saying they believe in a voluntary compliance model. We tried to see if the Attorney General's office is interested. They don't seem to be moving on this file at all.

One of the things that an RCMP officer told this survivor was that they believe Pornhub MindGeek was exempt because of their terms and conditions, the consent that exists on their website, and I know you've raised issues of the vague nature of terms of consent on websites.

Do you believe that the fact that they have their own set of terms of consent would somehow absolve them from the Canadian privacy laws?

Mr. Daniel Therrien: I'll be careful because we're investigating.

I'll just note the general principle that consent is generally required to collect, use and disclose personal information under Canadian private sector privacy laws, and even if consent is given, there's a further rule that provides that even if consent is provided, a company cannot collect, use and disclose information if a reasonable person would find that inappropriate.

Mr. Charlie Angus: Thank you very much for that. I really appreciate it. I understand that you are investigating, so I won't ask you any more on that. I just wanted to clarify that.

In the last Parliament, our committee sent the government a number of recommendations on strengthening the role of your office and ensuring that we get stronger protections for Canadians' privacy rights, the rights of our citizens. I have spoken with many people in the privacy and data field who have looked at this new legislation, Bill C-11, and they're raising concerns that this legislation may actually hinder a number of the objectives that we had laid out at our committee in the previous Parliament. One of those is the issue of meaningful consent.

You state that the consumer privacy protection act "leaves out an important facet of our current legislation, the idea that meaningful consent requires that the person giving it understands the consequences of what they are consenting to." You further state that you believe this law "would result in less consumer control than under the current law".

Can you explain your concerns?

● (1135)

Mr. Daniel Therrien: Yes. There's no question that Bill C-11 is a comprehensive and serious attempt to address privacy issues in the digital world, but at the most general level, we think that in order to provide adequate protection for privacy, the bill needs very significant changes.

Why? In part it's because we think that even though there are provisions on consent in Bill C-11, the ultimate impact would be less control for individuals, in part for the reason you suggest, that a requirement in the current law that individuals, consumers, understand the consequences of what they are being asked to consent to does not exist in Bill C-11 as drafted.

There are also important exceptions to consent in Bill C-11, some of which are appropriate but others much too broad. For example, there is an exception to consent where it is "impracticable" to obtain consent. We think that such an extremely broad exception to consent makes the rule hollow—so less control for individuals, more flexibility in Bill C-11 for organizations. We're not against additional flexibility for organizations per se, particularly when organizations want to use personal information for the public good or for a legitimate public interest, but we think additional flexibility should come with additional accountability.

Mr. Charlie Angus: I see. I'm running out of time here, but I just wanted to clarify that. I know that there has been a real concern, certainly under section 18, about the broad nature of so-called business activities and whether or not it's better to establish a fiduciary responsibility that imposes the duties of loyalty and of care when personal information is collected, particularly when we're dealing with information about people's racial and ethnic origins, philosophical beliefs, religious beliefs or their biometrics or genetics.

Do you think we need to have a much clearer definition of the obligation to protect this information?

Mr. Daniel Therrien: In brief, yes.

We think that part of the solution is, yes, to give additional flexibility for companies to use information for legitimate business purposes but within a privacy law that has a human rights foundation. That ultimately would be the most significant protection given to consumers.

Mr. Charlie Angus: Thank you.

The Chair: Thank you, Mr. Angus.

I'm going to turn to Monsieur Gourde for the next round of questions.

[*Translation*]

Mr. Jacques Gourde (Lévis—Lotbinière, CPC): Thank you, Mr. Chair.

Mr. Commissioner, thank you for being with us again today. It's always a pleasure to have you here.

You've told us that, under your mandate, you must respond to all complaints, but that you don't have the discretion to refuse some of them.

What kinds of complaints wouldn't warrant a review by your office?

Mr. Daniel Therrien: Before answering the question directly, I would like to remind committee members that, in other jurisdictions, this discretion is granted to agencies that are equivalent in nature to my office. The purpose is to ensure that these offices aren't flooded with complaints, which would prevent them from playing a proactive role. The goal is not to reject applications, but to be able to do all of our work.

Getting back to your question, it comes back to a question of risk assessment. It's not necessarily that complaints have no merit, but there are levels of risk among the complaints that are sent to us. For example, there are some complaints that involve only one person. For the latter, it is very important, and I fully agree that we must give everyone access to a justice system. However, if we have to choose between investigating a complaint whose outcome is only going to affect one person or dealing with another complaint whose resolution may establish a principle that will affect a large part of the population, in this case, unfortunately, we have to go with the second one.

● (1140)

Mr. Jacques Gourde: That is absolutely laudable.

The growing use of technology was also discussed. I'm trying to get a handle on that.

We know that technology can expedite some cases, but it's still going to take a human being to give advice and write some reports.

Can you shed some light on how technology can expedite these complaints?

Mr. Daniel Therrien: You're right. Ultimately, it takes a human being to analyze the file and respond to the complainant.

The technology is used primarily in the triage process. Currently, we have an obligation to deal with every complaint, but we don't process them all in the same way. Some we investigate thoroughly and some we investigate in a more expedited manner. One of the things we have is an early resolution process.

Technology can help us make an initial triage between complaints that should be resolved quickly and those that require further investigation. At the end of the day, however, in both cases, even the early resolution case, there is someone who needs to look at the file and respond to the complainant.

Mr. Jacques Gourde: Certainly, with the rise of all the new technology platforms, we're really on the fast track, if you will. Our work in Parliament has changed a lot in the space of eight or nine months, and it has to be similar to the office of the commissioner.

This method of operation exposes us to the risk of inadvertent or accidental disclosure of confidential information that concerns the public.

You talked a lot about public awareness. Does that entail telling Canadians to be more careful about certain things so that their identities are not disclosed, or do you have a broader objective?

Mr. Daniel Therrien: The outreach component includes this aspect, but it encompasses many others.

Technology is a complex area for a lot of people. For many people, it's difficult to understand the privacy risks they have to manage unless they have a minimal understanding of the basics of technology and personal information handling.

That being said, we are aware of the terms of use of websites, and we try to do what we can about it, but these terms are very complex, and there's a limit to what we can do. Still, we try to educate people about how the technology works and how it affects their personal information so they can make the most informed decisions possible.

[*English*]

The Chair: Thank you, Mr. Gourde.

We're going to turn to Mr. Sorbara for the next questions.

Mr. Francesco Sorbara (Vaughan—Woodbridge, Lib.): Thank you, Chair.

Good morning, everyone, and welcome, Privacy Commissioner.

In my time today.... I know we're focusing on the main estimates, but what's crucial for me is that your office has the pertinent resources for you to effectively undertake your job and your mandate. That's what's important to me, so on that level those are my thoughts.

I want to move on to something in terms of.... I've read about and followed your office very closely since joining this committee late last year. We just listened to the study that Mr. Angus referred to. When it comes to meaningful consent, this document from May 2018 says:

> Meaningful consent is an essential element of Canadian private sector privacy legislation. Under privacy laws, organizations are generally required to obtain meaningful consent for the collection, use and disclosure of personal information. However, advances in technology and the use of lengthy, legalistic privacy policies have too often served to make the control—and personal autonomy—that should be enabled by consent nothing more than illusory. Consent should remain central, but it is necessary to breathe life into the ways in which it is obtained.

Can you comment on that introductory paragraph?

I read your March 25, 2021 speech, and I read the Clearview AI information put forward. I still can't believe it stated that “Canadian privacy laws do not apply to its activities because the company does not have a 'real and substantial connection' to Canada”, even though it collected three billion images of Canadians and came up with that data.

Can you elaborate on meaningful consent, and how we need to balance that between consumer objectives, business objectives and individual objectives?

● (1145)

Mr. Daniel Therrien: Obviously, it's a very broad question. I will try to do justice to it in a few seconds or minutes.

Consent is a fundamental aspect of the current law, PIPEDA, and it will continue to have a central role under the CPPA under Bill C-11, so there is a place for consent in privacy in 2021. There need to be some rules to make sure that when consent does work, it is obtained in a meaningful way. In my view, that means, in part, to ensure that the consumers who provide consent have a good idea of what they are consenting to, which is not obvious. That's where consent does work.

As I was saying in the documents you were referring to, given where we are with digital developments, there are many situations, a growing list of situations, where consent does not really work, particularly when you think of artificial intelligence, for instance, where the purpose of the technology is to use information for purposes other than that for which it was obtained. That's not really conducive to consent being an adequate means to protect privacy.

Given where we are in 2021, and the following years, there is a role for consent, but we also need to have laws that acknowledge that consent will not always work. Then we need to find an adequate means of protecting privacy absent consent. That's where the real difficulty, I think, lies in the discussion of these issues, particularly with Bill C-11.

Bill C-11 has many more exceptions to consent, some appropriate, others too broad in our view. How do you protect privacy if consent is not the preferred means of protecting it? We propose a human rights approach to privacy protection. Other models are proposed, such as the fiduciary model that Mr. Angus was referring to.

The extremely difficult challenge ahead of Parliament in the next few months is to determine where consent does not work—and it does not always work—and what would be a good model to continue to protect privacy adequately absent consent.

Mr. Francesco Sorbara: Mr. Chair, if I can just finish off, because I know—

The Chair: You have but seconds, so if it's a short question....

Mr. Francesco Sorbara: This discussion is important to 38 million individuals in this country because this is individuals' data. This is not anyone else's data. This is individuals' data. That's the way I view this issue. We need to make sure that we get the balance right, but we also need to make sure that consumers, Canadian citizens, are protected. That is my fundamental belief.

Thank you for that answer, Commissioner.

Mr. Daniel Therrien: Thank you.

● (1150)

The Chair: We're going to turn to Monsieur Fortin now for the next two and a half minutes.

Monsieur Fortin.

[*Translation*]

Mr. Rhéal Fortin: Thank you, Mr. Chair.

Mr. Therrien, we've obviously only scratched the surface, but given everything that's just been said, how would you rate Canada, relative to other countries, in terms of privacy and protection of personal information?

I'd like you to give me your thoughts on this and to do some kind of comparative analysis in two minutes.

Mr. Daniel Therrien: Canada was once a leader in privacy protection, but unfortunately, that is no longer the case. Many countries, not only in Europe, but also in South America and Asia, such as South Korea and Singapore, are very innovative. They have laws that protect privacy better than Canada's. Again, I think it's important that the bill, which could be passed by the House in the coming months, allow Canada to catch up with other countries, which have managed to innovate, in terms of economics.

It is often said that overly stringent privacy protections inhibit innovation. Germany, South Korea, Singapore, and several other countries demonstrate very clearly that it is possible to have laws that protect privacy very well and also enable innovative economies. In fact, I would argue that better privacy laws increase consumer confidence, which is a factor that helps to stimulate a country's economy. I definitely see a connection between privacy, confidence and economic growth.

Mr. Rhéal Fortin: Why do you think Canada lost its leadership role in this area?

Mr. Daniel Therrien: I don't think I'm the best person to answer your question.

Mr. Rhéal Fortin: All right.

In this case, what do Germany and South Korea have that we need to look at?

[*English*]

The Chair: Mr. Fortin, your time is up. You'll have a chance to speak to the commissioner again when we start the next round in the next hour of the meeting.

Mr. Angus, we're going to turn now to you, for what I think will be the final questions of this hour. Then, we'll suspend and hear from the commissioner again.

Mr. Charlie Angus: Thank you so much.

I want to begin by saying that I am in complete agreement with my colleague, Mr. Sorbara, on the importance of getting Bill C-11 right, because it is about the rights of 38 million Canadians, and we all have that obligation.

Our committee previously brought forward a number of recommendations about the order-making powers of the Privacy Commissioner as well as the need to be able to levy huge fines. The vast majority of infringements on privacy we believe are accidental or without malice, but we do have some bad operators. We had Facebook say they didn't feel they had to follow Canadian law. We certainly see the same instance with Clearview AI, so the need to give you more tools was clear.

What concerns me, when I look at Bill C-11, is this idea of creating this regulatory tribunal that these companies could then go to about a decision.

I'd like to ask you, number one, whether we have any example of this kind of regulatory tribunal that can override a privacy commissioner's decision in any other jurisdiction, and how you feel about it. You state you believe that this tribunal would encourage companies to choose a route of appeal rather than finding common ground with the Privacy Commissioner's decisions, and it would actually delay and obstruct justice for consumers and privacy rights.

Could you give your thoughts on this regulatory tribunal balloon that has been floated by the government?

Mr. Daniel Therrien: I am concerned with the creation of this additional layer in the process. I'm concerned, obviously, not because I'm concerned with the issue of fairness towards companies who would be the subject of order-making. I totally get the point that it is important that the system as a whole provides fairness to both complainants and companies. However, to our knowledge, there is no other jurisdiction that has this additional layer between the Privacy Commissioner and the courts. We think that the courts are perfectly capable of reviewing our processes to ensure that companies are dealt with fairly.

The end result of the creation of this tribunal, as I said and as you noted, is that rather than having a conversation between us and a company where, at the first opportunity, we try to make things right, companies would be encouraged to use these avenues of redress, which would considerably lengthen the process and which would be a huge issue for citizens.

● (1155)

Mr. Charlie Angus: Thank you very much.

The Chair: Thank you, Mr. Angus.

Thank you, Commissioner Therrien. We appreciate the testimony you have provided in this first hour as we review the estimates.

We are going to suspend now, colleagues, before the second hour. In the second hour, of course, we're going to have the commissioner again, but we have to change out some of the additional witnesses.

We will now suspend for five minutes.

● (1155)

(Pause)

● (1200)

The Chair: I'm calling this meeting back to order.

For the second hour of this meeting, we're launching our study on facial recognition software and concerns related to it. Today we have the commissioner, who has agreed to remain here for an additional hour so that he can answer some questions as we launch into the investigation of this matter.

Thank you, Commissioner, for remaining with us.

We also have Mr. Homan, who is remaining with us as well, and Lara Ives, who is the executive director of the policy, research and parliamentary affairs directorate. Thank you so much for being here. Finally, we have Regan Morris, who is joining us as legal counsel.

Thank you as well for being here, Commissioner.

I'll turn it back to you for an opening statement to allow you to begin the discussion. Then we'll have questions for you.

Mr. Daniel Therrien: Thank you again, Mr. Chair.

[*Translation*]

Facial recognition technology has become an extremely powerful tool that, as we saw in the case involving Clearview AI, can identify a person in a bank of billions of photos or even among thousands of protesters. If used responsibly and in appropriate situations, it can provide significant benefits to society.

In law enforcement, for example, it can enable police to solve crimes or find missing persons. However, it requires the collection of sensitive personal information that is unique to each individual and permanent in nature. Facial recognition technology can be extremely privacy invasive. In addition to promoting widespread surveillance, it can produce biased results and undermine other human rights.

The recent Clearview AI investigation, conducted jointly with my counterparts in three provinces, demonstrated how facial recognition technology can lead to mass surveillance and help treat billions of innocent people as potential suspects. Despite our findings that Clearview AI's activities violated Canadian privacy laws, the company refused to follow our recommendations, such as destroying the photos of Canadians.

In addition, our office is currently investigating the Royal Canadian Mounted Police, or RCMP, use of Clearview AI technology. This investigation is nearing completion. We are also working with our colleagues in all provinces and territories to develop a guidance document on the use of facial recognition by police forces. We expect to release a draft of this document for consultation in the coming weeks.

[*English*]

The Clearview case demonstrates how citizens are vulnerable to mass surveillance facilitated by the use of facial recognition technology. This is not the kind of society we want to live in. The freedom to live and develop free from surveillance is a fundamental human right. Individuals do not forgo their rights merely by participating in the world in ways that may reveal their face to others or enable their image to be captured on camera.

The right to privacy is a prior condition to the exercise of other rights in our society. Poorly regulated uses of facial recognition technology, therefore, not only pose serious risks to privacy rights but also impact the ability to exercise such other rights as freedom of expression and association, equality and democracy. We must ensure that our laws are up to par and that they impose limits to ensure respect for fundamental rights when this technology is used.

To effectively regulate facial recognition technologies, we need stronger protections in our privacy laws, including, among other things, a rights-based approach to privacy, meaningful accountability measures and stronger enforcement powers. The federal government recently introduced two proposals to modernize our privacy laws. These are important opportunities to better regulate the use of facial recognition and other new technologies.

Last November, the Department of Justice released a comprehensive and promising consultation paper that outlined numerous proposals to improve privacy legislation in the federal public sector. It proposes enhanced accountability requirements and measures aimed at providing meaningful oversight and quick and effective remedies. It also proposes a stronger collection threshold, which would require institutions to consider a number of factors to determine if the collection of personal information is “reasonably required” to achieve a specific purpose, such as ensuring that the expected benefits are balanced against the privacy intrusiveness, so that collection is fair, not arbitrary and proportionate in scope.

In the private sector, Bill C-11 would introduce the consumer privacy protection act. In my view, as I stated in the last hearing, that bill requires significant amendments to reduce the risks of facial recognition technology. The significant risks posed by facial recognition technology make it abundantly clear that the rights and values of citizens must be protected by a strong, rights-based legislative framework. The Department of Justice proposes adding a purpose clause to the Privacy Act that specifies that one of the key objectives of the legislation is "protecting individuals' human dignity, personal autonomy, and self-determination", recognizing the broad scope of the right to privacy as a human right.

Conversely, Bill C-11 maintains that privacy and commercial interests are competing interests that must be balanced. In fact, compared with the current law in the private sector, PIPEDA, the bill gives more weight to commercial interests by adding new commercial factors to be considered in the balance without adding any reference to the lessons of the past 20 years on technology's disruption of rights.

Clearview was able to rely on the language of the current federal act, PIPEDA, to argue that its purposes were appropriate and the balance should favour the company's interests rather than privacy. Although we rejected these arguments in our decision, some legal commentators have suggested that our findings would be a way to circumvent PIPEDA's purpose clause by not giving sufficient weight to commercial interests. Even though we found that Clearview breached PIPEDA, a number of commentators, including the company but not limited to the company, are saying that we actually misapplied the current purpose clause.

If Bill C-11 were passed in its current form, Clearview and these commentators could still make these arguments, buttressed by a purpose clause that gives more weight to commercial factors. I urge you to make clear in Bill C-11 that where there is a conflict between commercial objectives and privacy protection, Canadians' privacy rights should prevail. Our submission analyzing this bill makes specific recommendations on the text that would achieve this goal.

● (1205)

[*Translation*]

Demonstrable accountability measures are another fundamental mechanism to protect Canadians from the risks posed by facial recognition. Obligations to protect privacy by design, conduct privacy impact assessments, and ensure traceability with respect to automated decision-making are key elements of a meaningful accountability framework. While most of these accountability measures are part of the Department of Justice's proposals for modernizing public sector law, they are all absent from Bill C-11.

Efforts to regulate facial recognition technologies must also include robust compliance mechanisms that provide quick and effective remedies for individuals.

Our investigation into Clearview AI revealed that the organization had contravened two obligations under Canadian privacy law. On the one hand, it collected, used and disclosed biometric information without consent, and for an inappropriate purpose.

Remarkably—and shockingly—the new administrative penalty regime created by Bill C-11 would not apply to these and other important violations of the legislation. Such a penalty regime renders meaningless laws that are supposed to protect citizens.

I therefore urge you to amend the bill to remedy this fundamental flaw.

In conclusion, I would say that the nature of the risks posed by facial recognition technology calls for collective reflection on the limits of acceptable use of this technology. These limits should not be defined only by the risks associated with specific facial recognition initiatives, but by taking into account the aggregate social effects of all such initiatives over time.

In the face of ever-increasing technological capabilities to intrude on our private lives, we need to ask ourselves what are the expectations we should be setting now for the future of privacy protection.

I thank you again for your attention.

I welcome any questions you may have.

● (1210)

[*English*]

The Chair: Thank you, Commissioner.

Colleagues, I want you to be aware that we should be expecting a vote in the House of Commons. The bells may start as early as 12:35, so unless there's an objection at that point in time, I will assume there's unanimous consent to continue with the questions. We will ensure that sufficient time is allowed for members to log in, so that at 1:05, when the voting begins, members are logged in and able to vote.

Unless there's an objection from committee members, we'll continue with the questioning.

We will begin with Mr. Carrie.

Mr. Colin Carrie: Thank you very much, Mr. Chair.

Monsieur Therrien, I want to thank you for your wisdom. With Bill C-11 coming down the pipe, it's so important that we lean one way versus the other way.

I know with facial recognition, when you first see it, it's so cool. We all heard about the issue with Cadillac Fairview, the shopping mall issue. Maybe we'll get to that today, but even sites like Facebook, they have these tag suggestions and they insert them as default settings. Theses sites are collecting our data, our faces, and many times people are totally unaware of it. That's where I want to start our conversation today.

I come from Oshawa. Oshawa is one of those communities that historically built cars and sent people back and forth across the border, things along those lines. I want to talk to you a little bit about the international utilization of facial recognition. I've heard that border efficiencies could be improved. I was wondering if you could comment on the opportunity, perhaps, for these opt-in, opt-out options if we're going back and forth across borders for business or as individuals.

Are there any international conversations about the right to delete and destroy information that may be gathered from Canadians as they cross borders into other countries?

Mr. Daniel Therrien: I will answer the question by going back to the point that I made early in my statement that facial recognition can serve society. At the border, for instance, it can greatly accelerate and make more efficient the triage of individuals who wish to cross the border. In police and law enforcement, it can facilitate the resolution of crimes or find missing persons.

I would not start from the premise that facial recognition should be banned completely or even in certain sectors completely, as in law enforcement, for instance. It can be useful, but it is very special in that it collects the attributes of a person that are immutable. If there's a breach of that information in the company or the government department that has collected it, you cannot change your biometrics like you can change a password. It is immutable and that means that this particular technology needs to be regulated very rigorously so that it does bear fruit and provides benefits to society without creating nightmares for individuals who, again, can no longer protect their privacy if someone uses their biometrics, including facial recognition, for nefarious ends.

That would be my answer for the border.

● (1215)

Mr. Colin Carrie: It's a good answer. I sat on the international trade committee, and we just completed the CUSMA, agreement. As we move through this process with the framework of our trade agreements, do you have any thoughts about ensuring Canadians have their rights looked after when we enter into these trade agreements? Do you think CUSMA has sufficient protections in it, basically?

Mr. Daniel Therrien: That's a huge issue.

Mr. Colin Carrie: I know. That's why you get the big bucks.

Mr. Daniel Therrien: When the time comes to share personal information outside Canada, and still do it in a privacy-protected way, I think there needs to be additional safeguards to those that apply within Canada, because the risks to privacy are not the same when the data leaves the country. This does not mean that we should live in a data localization world where the data of Canadians does not leave Canada, but I think it's important to acknowledge that the risks are higher when the data leaves Canada.

Then of course comes the question of what additional protection should come in these situations, because we live in an interconnected world. We're neighbour to the United States. It's a reality that data often moves to the United States. I'm afraid I won't give an opinion on whether CUSMA adequately does that. Whether data leaves Canada is not a benign issue, and we should think hard about what additional protections should be created by Parliament to ensure that privacy continues to be protected when data does leave Canada.

Mr. Colin Carrie: That's excellent. Thank you very much.

Maybe another time I'll ask you about China and that might be a more interesting conversation.

Thank you very much, Mr. Commissioner.

The Chair: Thank you, Mr. Carrie.

We'll go to Mr. Dong next.

Mr. Han Dong (Don Valley North, Lib.): Thank you, Chair.

I want to thank the commissioner and his staff for agreeing to stay longer to answer some very important questions. I had some questions prepared, but after your opening statement I have a few others added to the list.

First, there has been a lot of discussion, our committee included, with regard to facial recognition technology and whether it could potentially be more harmful to racialized communities. In your findings, is there any evidence to support that?

Mr. Daniel Therrien: There's certainly a lot of literature and analysis by academics and experts on this question. We have not actually made findings on this in the context of Clearview AI, but we have read a lot of very credible scientific research that is concerned with whether the technology is sufficiently precise, particularly in the case of racialized communities, to be used in a way that does not violate privacy or other rights like equality rights. There are concerns about this.

From a privacy perspective, the issue would be that facial recognition needs to be used in a way where accurate information is collected. The principle of accuracy is one of the important privacy principles. Again, there is a lot of literature to the effect that, for racialized communities, the information collected may not always be accurate, depending on the technology in question.

● (1220)

Mr. Han Dong: Without any empirical evidence that facial recognition technology could be harmful, particularly to a racialized community, is there anything in Bill C-11 that we can do to provide a guardrail to make sure that the vulnerable communities don't get harmed as facial recognition technology develops?

Mr. Daniel Therrien: Bill C-11, as mentioned, does not have a human rights approach to the privacy law in question. It would be very beneficial if the proposed CPPA had a human rights foundation because then the principle of accuracy that I just alluded to could be used to ensure that potential discrimination against populations in the use of facial recognition would be part of our remit to ensure that, under privacy principles, technology that would result in discrimination would be found contrary to privacy.

I'll say that some would argue that these issues should be addressed through human rights legislation. Certainly, that's a credible point. I would say that, in the virtual world as in the physical world, the fact that there is some overlap in the jurisdiction of regulators here, as between my office and the Canadian Human Rights Commission, is not a bad thing as long as the regulators speak to one another, are efficient and benefit from each other's expertise. Our model would be to have a human rights approach to privacy law.

Mr. Han Dong: I see. That's a very good point.

You mentioned that the facial recognition technology could be beneficial to our law enforcement system. Do you have any thoughts on what processes are in place or should be in place to ensure that the Government of Canada has the public's trust in utilizing facial recognition?

Mr. Daniel Therrien: I'll say something on the general level because we have not completed our investigation on the RCMP. The issue you raise is central. Obviously, whether it's companies or government departments—including law enforcement agencies—that use facial recognition, they should have processes ahead of the implementation of these technologies to assess the impact that they may have in order to ensure that privacy is respected. That's a central part, I think, before the technology is actually put into place.

Mr. Han Dong: I don't mean to cut you off, but I want to get my next question in.

Does your office currently have enough resources to dive deeper on the algorithm, data storage or process to access data? Does your office currently have enough resources to do this type of investigation? It's not just with money. I'm also talking about technically—

Mr. Daniel Therrien: You mean the nature of our expertise.

Mr. Han Dong: Yes.

Mr. Daniel Therrien: We do have a group of technologists. Roughly 12 individuals who are experts in technology assist in our policy development and investigative activity. In terms of the kinds of people, I think we have the right people. Then there's the question of how many resources, and that was the subject of some discussion in the last hour.

Mr. Han Dong: You mentioned a partnership between the federal government and the provincial government. In your mind, what is the jurisdictional divide between the provincial and federal systems?

Mr. Daniel Therrien: Do you mean as to facial recognition?

● (1225)

Mr. Han Dong: I mean the legislative aspect of facial recognition.

Mr. Daniel Therrien: It is the same jurisdictional divide as for other technologies. There's a federal private sector law that governs the private sector when the provinces have not legislated. Obviously, the provinces would legislate the conditions under which their own officials would use facial recognition, so the same jurisdictional issues would arise here as with other technologies.

The Chair: Thank you, Mr. Dong.

We'll turn to Monsieur Fortin now for the next round of questions.

Monsieur Fortin.

[*Translation*]

Mr. Rhéal Fortin: Thank you, Mr. Chair.

Mr. Therrien, the more I listen to you, the more I realize that studying Bill C-11 is quite a chore. The privacy situation is really concerning. It's something that everyone is concerned about, here in Quebec at least, and I'm sure it's the same in the rest of Canada, if not the entire planet.

I'm a little concerned about what you're telling us with respect to Bill C-11, which might not cover all the angles, some of which would be quite important. I note, among other things, your caveat about facial recognition data being immutable. Once we have that data, it will be there for life. I also note the issue of exchanges between countries, where we must be even more careful, because the protections are not the same in all countries. In this day and age, with more and more trade between countries, I guess you have to be more and more careful, and put more time and effort into it. Those are some of the concerns we have.

When Bill C-11 was being developed, did you intervene? Was the Conflict of Interest and Ethics Commissioner called in to advise the minister, and did he try to include the various safeguards that you feel are missing from the current version of the bill? Have you prepared a report or other document?

Mr. Daniel Therrien: We have produced several public reports recommending that federal legislation reform be approached from the angle of protecting privacy rights. We have submitted several reports to Parliament along these lines. We had some exchanges with officials at the Department of Innovation, Science and Economic Development, but we never saw the bill before it was introduced. Cabinet secrecy was invoked to limit our discussions with the department during the development of the bill. However, the department was still aware of our position, through our public reports presented in Parliament and elsewhere.

I have to say that I am disappointed that the bill that has been tabled departs so broadly from what the regulatory agency believes is necessary for adequate privacy protection.

Mr. Rhéal Fortin: If you were asked to do so, would you be able to propose a series of amendments that would ensure that citizens' privacy is better protected? Would you consider making a concrete proposal?

Mr. Daniel Therrien: We did more than just consider it, we prepared a brief.

Following the bill's passage in November, we worked very hard to analyze it from every angle. Members who wish to do so can review this brief, which analyzes the bill and makes several recommendations to amend it.

Mr. Rhéal Fortin: I, for one, would like to, and I believe everyone here wants to as well. It would surprise me if anyone said otherwise.

Would it be possible to send us a copy, Mr. Therrien?

Mr. Daniel Therrien: If the committee requests it, I will be more than happy to do so.

Mr. Rhéal Fortin: Mr. Chair, on behalf of my colleagues, if they agree, I am formally requesting that we be sent a copy of this brief.

● (1230)

[*English*]

The Chair: I think the commissioner has said that he'd make it available. As a committee, I think we would be happy to accept anything the commissioner would provide for us.

[*Translation*]

Mr. Rhéal Fortin: Thank you, Mr. Chair.

Thank you, Mr. Therrien.

Mr. Therrien, you were saying that the Clearview AI investigation was almost complete. When can we expect to receive the report?

Mr. Daniel Therrien: The Clearview AI investigation is complete.

The investigation that is coming to a close, and is not quite finished yet, is about the RCMP and its use of Clearview AI technology. We should be able to release that report in the next few weeks.

Mr. Rhéal Fortin: If I understand correctly, it will be before the summer adjournment. Is that correct?

Mr. Daniel Therrien: Yes, that's right.

Mr. Rhéal Fortin: We don't have much time, as you know. So I'm going to go back to the question I asked you earlier about other countries that are leaders in privacy protection.

You mentioned Germany, South Korea and Singapore. What makes them different? How are they ahead of Canada in this regard?

Mr. Daniel Therrien: It depends on the country. In Europe and elsewhere, such as in some Latin American countries, Japan, and, if I am not mistaken, South Korea, the approach we suggest exists, which is to have the protective provisions enforced within a human rights framework.

Then there are considerable penalties so that consumers can have confidence that their data is being handled with respect for their privacy. As one of the committee members said earlier, many companies are acting in a compliant manner, but some really need incentives. So there need to be significant penalties, and there are penalties in their legislation.

I would remind you that failures like Clearview AI's would not be subject to administrative penalties under the provisions of Bill C-11, which is rather hard to understand.

Mr. Rhéal Fortin: That is disappointing.

Mr. Daniel Therrien: It's very hard to understand.

There need to be significant penalties, a rights-based approach, and more flexibility in how data is used. This must go hand in hand with greater corporate accountability. Among other things, this means that the regulatory agency can, not arbitrarily, but by being focused on its assessment of the environment, do proactive audits and not wait until there is a privacy breach. A proactive aspect is very important to properly protect consumer privacy, in my opinion.

Mr. Rhéal Fortin: Are you optimistic, Mr. Therrien?

[*English*]

The Chair: Thank you, Mr. Fortin.

We're going to turn to Mr. Angus.

Mr. Charlie Angus: Thank you very much.

Mr. Therrien, when we first learned of the Clearview AI case, it seemed to be the worst possible scenario. Here we had this company that scraped millions of photos of Canadians without their consent—our kids' birthday parties, our backyard barbecues, us at work—and then created a database that they were selling to all manner of organizations.

They claim it was for police, but we know that individual police officers had it without oversight. We know that a billionaire, John Catsimatidis, used it to target his daughter's boyfriend. You launched an investigation. Clearview AI's attitude was “Too bad, so sad. You're just Canadians and we don't even feel obligated to follow the law.”

We had a new law, Bill C-11, come in. My understanding, my gut feeling, was that Bill C-11 would fix these things so that we would have more powers and we'd be able to target these companies to make them respect the law. Are you telling us that under Bill C-11 the weight of support would actually go to rogue outliers like Clearview AI over the rights of citizens?

Are you saying that, on the monetary penalties we've been told about that would ensure compliance, a company like Clearview AI would be completely exempt from that? Is that what we're seeing under this new law?

Mr. Daniel Therrien: Two main mechanisms are relevant to Clearview's situation under CPPA.

The first one is the purpose clause—proposed section 5—of the CPPA, which confirms the PIPEDA's approach to balance commercial interests with privacy considerations. That clause does not say that privacy is a human right. That clause adds a number of commercial factors compared to the current law. There would be a balancing exercise, with the likelihood of greater weight given to commercial factors than under the current PIPEDA. That's point one.

Point two is that assuming it would be inconsistent with the CPPA for Clearview to do what they did, there's an administrative penalty scheme under Bill C-11 and a criminal penalty scheme under Bill C-11. The administrative penalty scheme is limited to an extremely narrow slice of violations of the CPPA. These violations have to do with a form of consent with the understanding requirement that I referred to before—with whether Clearview had the right balance between commercial interests and human rights. All of that cannot be the subject of administrative penalties under the CPPA.

In order for penalties to apply, the office would have to first make a finding, which would take about two years. Secondly, they would make an order. The penalty would be excluded. The tribunal would sit in appeal of our order, assuming the company would still not comply with the order. If the company would not comply with an order several years after it has been made, then it would be the subject of criminal penalties and the criminal courts would be involved.

The process that leads to penalties is very protracted. We think it's something like seven years after the fact, as opposed to what should be happening, which is that we should be able to impose penalties—of course subject to court review for fairness considerations vis-à-vis companies. We think the delay would be roughly two years in that model compared with the model in Bill C-11.

● (1235)

Mr. Charlie Angus: This is really important because I think most Canadians would agree that Clearview AI's situation was very concerning. We could see many more examples of this as this technology becomes more commonplace, yet we have legislation that seems to be going backwards. It's willing to protect Clearview AI rather than citizens.

I ask this because we have Bill C-10, which should have been a pretty straightforward bill about making the tech giants pay their part. Instead, it has turned into this legislative dumpster fire with the minister running around looking like a chicken with his head cut off. Our committee had brought forward really clear recommendations on the issue of privacy rights.

You're telling us, with Clearview AI, that this law is actually not taking the lessons we learned on issues like facial recognition and from the big data giants ignoring their obligations under Canadian law, but actually writing in more protections for that abuse because we're not looking at it in a human rights frame. Is that correct?

Mr. Daniel Therrien: I think very significant amendments to Bill C-11 should be made to adequately protect privacy.

Mr. Charlie Angus: Thank you.

I just want to follow up on the RCMP investigation. The RCMP refused to tell the Canadian public whether they were using this technology at all.

Are you looking at laws that would ensure the compliance of our police services using companies like Clearview AI?

Mr. Daniel Therrien: My report will address that theme generally. I'll leave it at that.

Mr. Charlie Angus: Thank you.

The Chair: Thank you.

We'll turn to Monsieur Gourde now for the next round of questions.

[*Translation*]

Mr. Gourde, you have the floor.

Mr. Jacques Gourde: Thank you, Mr. Chair.

Commissioner, we have a sense that reality will be stranger than fiction given these new applications. I think Canadians are relatively worried about living in a world where you can be recognized and filmed at any time and at any place, especially when you live in urban areas where there are cameras on every corner and in virtually every building.

Where will the potential abuses be committed in this new life we will soon be living? In fact, it may have already begun.

● (1240)

Mr. Daniel Therrien: We've seen an example of this with Clearview AI. To socialize with friends and family, users innocently use social media with no idea that the information they provide, including their photos, may be collated by a company like Clearview AI, which uses the data for so-called police investigations or, as mentioned, to conduct private investigations of individuals.

You mentioned that the presence of surveillance cameras in some public places also poses a significant risk. I would add, again, that facial recognition can play an important role, particularly in providing security in relation to certain events. The use of facial recognition in public places is a sensitive matter, but I wouldn't say it should be banned altogether.

I strongly encourage you to ask other witnesses to come where they think the problems lie. For my part, I would answer that it is in several places. I don't think you can regulate the whole situation. You have to look at it from a values perspective, and that again brings me back to the question of anchoring legislation in a human rights framework. This is more apparent in the case of the Department of Justice proposals than in the case of Bill C-11. Values are important. Respect for human rights is important. Second, there should be mechanisms to balance commercial interests and human rights, and these mechanisms should be better than those in Bill C-11. We will forward our recommendations to you in this regard.

I would add as a final point that right now our laws in Canada and in many countries—it's not the case everywhere—are said to be technology neutral. That means that the principles apply equally across the board, regardless of the type of technology, including biometrics and facial recognition. There are great advantages to this, and I am not suggesting that this aspect of our laws should be set aside. I think one of the things that you should be looking at is—and your question is very relevant to this—whether there is a need to circumscribe facial recognition activities. This would mean either prohibiting them or subjecting some of them to particularly strict regulation. In this regard, I refer you to a draft regulation on artificial intelligence, published in April by the European Commission. In it, certain prohibited practices are defined, including the use of live facial recognition in certain public places, except for exceptional cases, such as the investigation of major crimes or acts of terrorism.

This is a mixture of general principles about how to balance commercial or governmental interests and human rights on the one hand, and laws of general application on the other. In my view, we need to ask ourselves if there is a case to be made for some specific rules that would either prohibit or strictly regulate this technology; it presents particular risks, because biometric data is permanent.

Mr. Jacques Gourde: What can Canadians do to protect themselves in extreme cases where their privacy has been breached or technology has been used improperly?

Recently, there were cases in Montreal. People had bought cameras online and installed them in toilets and showers. That is happening, and apparently, those types of tiny cameras are readily available and easy to hide. People are engaging in voyeurism, and those images can end up anywhere.

What recourse should people have?

● (1245)

Mr. Daniel Therrien: It's pretty clear that—

[*English*]

The Chair: Thank you, Mr. Gourde.

Mr. Gourde's time has expired, but I'll allow you to answer the question, Commissioner.

[*Translation*]

Mr. Daniel Therrien: It's pretty clear that that type of use is unacceptable, even under the current privacy legislation. It's unacceptable. Penalties would be the answer in this case.

Deterring that kind of behaviour would require significant penalties, and neither the current act nor Bill C-11 sets out such penalties.

[*English*]

The Chair: Thank you.

Ms. Lattanzio, we'll turn to you.

Ms. Patricia Lattanzio (Saint-Léonard—Saint-Michel, Lib.): Thank you, Mr. Chair.

Thank you, Mr. Therrien, for your testimony this morning. It was quite informative.

What I'm drawing from it is that there's a constant need of striking a balance between individual human rights, public confidence and economic growth. It's going to be quite a difficult task, because technology is forever evolving and it's going at a very fast pace. In my opinion, a restudy is more than warranted as we do not know when we will get Bill C-11.

On the question of cross-border data, that's of interest to me because given the nature of cross-border data, as it flows, it adheres to international best practices and standards, which will be instrumental for ensuring Canadian competitiveness.

Is it correct to say—and I want to go back to that European notion you were talking about earlier—that the EU data protection regulation remains the international gold standard? How can Canada ensure equivalency with this regulation? That would be my first question.

Why is it in Canada's interests to retain the equivalency with the EU?

Mr. Daniel Therrien: The government certainly cited the desirability of Canada maintaining adequacy status in the EU as one impetus for Bill C-11. Indeed, maintaining adequacy is important. It allows data flows between Canada and the EU without specific mechanisms, like special contracts and the like.

Clearly, for Canada maintaining adequacy is helpful in order to maintain a freer flow of data between Canada and the EU. Beyond the EU, as I've said, we live in an interconnected world, and obviously, we have a neighbour to the south with whom we have very significant fundamental commercial relations, so data also needs to flow there.

I think that's all good, but we need to.... Hopefully, in the context of the review of Bill C-11, we can look at ways to allow these data flows, but in a way that recognizes that when data leaves Canada, the risks are higher.

I'm not advocating for ways to prevent these data flows, but certainly, in the submission you will now be able to read, we make certain recommendations on how to enhance the protection of personal information when it does leave Canada, while still allowing that.

Ms. Patricia Lattanzio: We will see these recommendations in the brief you spoke about earlier that you'll be filing. Is that correct?

Mr. Daniel Therrien: Yes.

Ms. Patricia Lattanzio: Okay.

You also spoke about the overlapping jurisdiction with the Human Rights Commission. What about the Competition Bureau of Canada? Your colleagues there are also grappling with the new and emerging privacy issues brought about by some of the changes in technology we're seeing, including the emergence of facial recognition software.

Can you describe the relationship between the two offices?

Mr. Daniel Therrien: Indeed, that's another relationship that's very important. I think we have a good relationship with the Competition Bureau. Again, as I said earlier, in the virtual world as in the physical world, it's normal to have a number of regulatory agencies that share different activities from different perspectives.

It's good to have both the Competition Bureau and the Office of the Privacy Commissioner. The important thing is to ensure that the law allows a certain sharing of information between these agencies, so that we can benefit from our respective expertise and also, from an operational perspective, we can divide files according to who's best placed to handle them.

At the general level, we need to be able to co-operate with other regulators, including the Competition Bureau. There are provisions in Bill C-11 to facilitate that, and that's a good thing. We look forward to further co-operation with the Competition Bureau and others.

● (1250)

Ms. Patricia Lattanzio: From a citizen perspective, how will the citizen be best guided as to where to place his or her complaint if we have overlapping jurisdictions between different offices?

Mr. Daniel Therrien: There should not be complete overlap. Maybe I should make that clear.

The Competition Bureau has jurisdiction over consumer protection and competition, and there is some overlap with us when personal information is involved. To that extent, I think we need to live with these overlaps, but the mandate of these various bodies should make it clear who is responsible for what.

I'm not advocating to play a role in competition law; the bureau is well placed to do that. However, privacy issues should be largely within our realm.

Ms. Patricia Lattanzio: You have—

The Chair: Thank you, Ms. Lattanzio. You are out of time, unfortunately.

We'll turn to Monsieur Fortin now for the next round of questions.

Monsieur Fortin, you have two and a half minutes.

[*Translation*]

Mr. Rhéal Fortin: Thank you, Mr. Chair.

Mr. Therrien, I gathered from your remarks that a number of departments can propose legislation with a potential impact on people's privacy.

Let's say a department proposes legislation with some privacy implications. Do you think a directive should apply to the department requiring it to obtain the Privacy Commissioner's approval beforehand? Wouldn't such a requirement ensure privacy was adequately protected?

Mr. Daniel Therrien: I completely agree that departments should consult our office beforehand when they are considering legislative or even administrative measures with significant privacy implications.

You used the word “approval”, but I think departments need to retain their responsibilities, as delegated. I think it's a very good idea for departments to consult us and for our office to provide opinions that will then inform government decision-making. However, in keeping with the principles of accountability, the government should ultimately be the one deciding what to bring forward because it is responsible for proposing legislation.

Mr. Rhéal Fortin: As I see it, Bill C-11, a pivotal piece of privacy legislation, is incomplete or ill-considered. We'll see. Quite a few deficiencies could have been avoided had you been involved in the legislative process from the outset. Wouldn't you say?

Mr. Daniel Therrien: Yes, we would have liked to be more involved. However, we recognize that making decisions is the government's responsibility at the end of the day.

Mr. Rhéal Fortin: I nevertheless think those decisions should be informed by the expertise of the Office of the Privacy Commissioner of Canada. That's just my opinion.

Mr. Daniel Therrien: That's my opinion as well.

● (1255)

Mr. Rhéal Fortin: Most folks have already provided their biometric information, if only for the purposes of a passport or cell phone. Previously, people would unlock their phones using a fingerprint scanner, and now they can do it through a facial recognition feature. As members of Parliament, we use a facial recognition system to cast our votes. I would say that just about every single person has inevitably shared their biometric information somehow.

Don't you think it's a bit too late to prevent the misuse of that information? Do you think it's still possible to get the situation under control, to curb the problem?

Mr. Daniel Therrien: It is indeed late, but technology isn't going to stop advancing. I think government and parliamentary institutions need to develop rules governing the use of that technology going forward.

Someone brought up how complex technology was. That is absolutely true, but I think it becomes a whole lot less complex when we commit to projecting our values in the legislation regulating that technology.

Yes, technology is complex, but our values are well-known. My recommendation is to ensure the legislation that regulates the digital space reflects our values as a society. That would be a great starting point.

Mr. Rhéal Fortin: We agree with you.

Thank you, Mr. Therrien.

[*English*]

The Chair: Thank you, Monsieur Fortin. You are out of time.

Mr. Angus, we'll turn to you now for the next two and a half minutes.

Mr. Charlie Angus: Thank you, Mr. Chair.

Mr. Therrien, one thing I thought was really profound in your findings against Clearview AI was that you said it would essentially subject the citizens of this country to a perpetual police lineup.

What we're talking about is not dystopian science fiction. We should know, as citizens, that when our children go to the mall, they aren't being photographed and put into a database; that racialized citizens are not being targeted on the streets where they walk; and that the right to go into a public place is a public right and we should not be profiled, targeted or put into some form of database for collection.

The Clearview AI case was a really good opportunity for Canada to get this right, because it was so egregious. What you're telling us is that the laws were written, in a way, to protect these outlier companies, ignoring the growing awareness that's happening internationally.

With Bill C-11, if the government is refusing to make the necessary changes to put a human rights frame on the rights of privacy, and if it is going to insist on protecting the interests of corporations that may not have the best interests of our citizens at heart, would we be better off with the status quo than putting more weight on the side of companies and outliers like Clearview AI?

Mr. Daniel Therrien: First, I would not ascribe motivation to those who have tabled Bill C-11, other than trying to balance commercial interests and privacy concerns and issues, and—

Mr. Charlie Angus: I fully understand that.

I'm just asking.... You say you're concerned that after Clearview AI, they would potentially have stronger legal power or ability to resist. That's my concern.

Mr. Daniel Therrien: That's my concern, as well.

Indeed, I think it is quite possible that a court, seized with a matter like Clearview AI, under CPPA, would not necessarily maintain the decision that we have made, in part because of the way the balancing clause of the CPPA is drafted. I find that extremely concerning, as well as the limited nature of administrative penalties under Bill C-11.

Mr. Charlie Angus: Thank you very much.

The Chair: Thank you, Mr. Angus.

Colleagues, we will move to adjourn shortly, but I just want to inform colleagues that we have two witnesses for the upcoming meeting. This Friday, we have—I'm just reminding myself, so I don't get it wrong—the Information Commissioner as well as the Commissioner of Lobbying confirmed, each for one hour.

Commissioner, thank you so much for joining us on these two important meetings, first on estimates, and then, of course, as we launch into the study on facial recognition technologies. We certainly appreciate your willingness to come and to be prepared to answer questions on both of those issues, as well as the willingness of our additional witnesses.

Colleagues, there are a few minutes left before the bells end, but I want to adjourn this meeting to allow members to be prepared to vote and to be logged in when that happens.

Again, Commissioner, thanks so much.