HOUSE OF COMMONS
CHAMBRE DES COMMUNES
CANADA

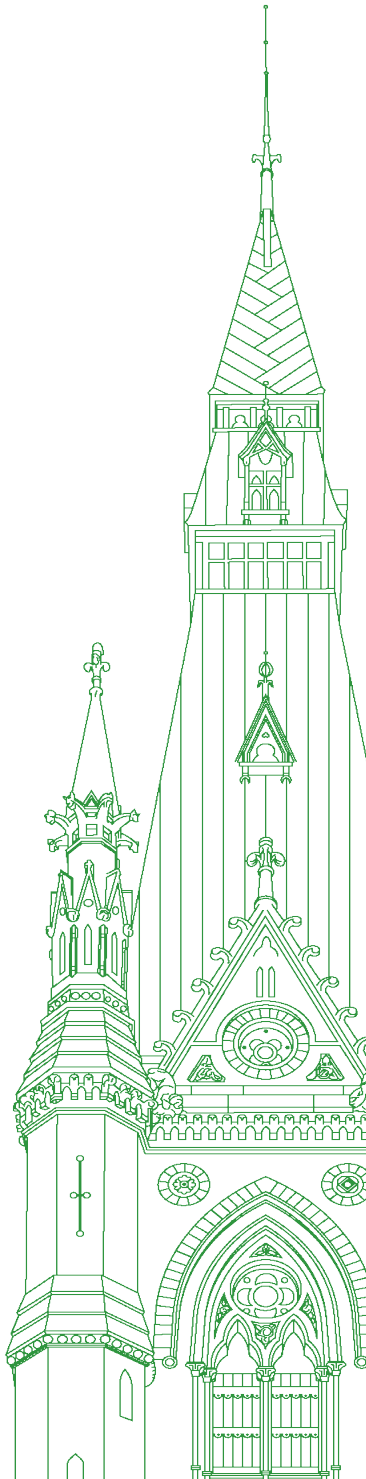
44th PARLIAMENT, 1st SESSION

Standing Committee on Access to Information, Privacy and Ethics

EVIDENCE

NUMBER 049

Monday, November 28, 2022



Chair: Mr. John Brassard

Standing Committee on Access to Information, Privacy and Ethics

Monday, November 28, 2022

● (1530)

[*Translation*]

The Chair (Mr. John Brassard (Barrie—Innisfil, CPC)): I call the meeting to order.

Welcome to meeting number 49 of the House of Commons Standing Committee on Access to Information, Privacy and Ethics.

[*English*]

Today's meeting is taking place in a hybrid format, pursuant to the House order of June 23, 2022. Therefore, members can attend in person in the room and remotely using the Zoom application.

Should any technical challenges arise, please advise me. Please note that we may need to suspend for a few minutes, as we need to ensure that all members are able to fully participate.

Pursuant to Standing Order 108(3)(h) and the motion adopted by the committee on Monday, November 14, the committee is commencing its study of privacy concerns in relation to the ArriveCAN application.

I would now like to welcome our witnesses today.

[*Translation*]

Mr. René Villemure (Trois-Rivières, BQ): For the benefit of the interpreters, I'd like to know whether the sound checks were done before the meeting.

The Chair: Were the sound checks done, Ms. Vohl?

The Clerk of the Committee (Ms. Nancy Vohl): It wasn't necessary to do sound checks for the witnesses appearing in person, here in the room.

In the second panel, one of the witnesses will be appearing by video conference, and we'll let you know then how the sound check went.

The Chair: Thank you.

[*English*]

I'd like to welcome our witnesses today.

From Digital Public, we have Bianca Wylie, who's a partner. As an individual, we have Mr. Matt Malone, assistant professor at Thompson Rivers University.

Ms. Wylie, the floor is yours, and you have five minutes for an opening statement. Thank you.

Ms. Bianca Wylie (Partner, Digital Public): Good afternoon. Thank you for the opportunity to speak to you about ArriveCAN today.

Our firm, Digital Public, does work focused on digital transformation, both in government and more broadly. I'm sharing thoughts today based on my experience working with software as a product manager and as a facilitator to support democratic process.

There is a long list of what went wrong with ArriveCAN. At the top of the list is the inequity in public service delivery it created and the damage it did to public trust in government, particularly during a public health crisis.

We can discuss the specific details of what went wrong together, but for the purpose of these short remarks, I'm going to share three proposals that may help us avoid replicating our ArriveCAN mistakes. The recommendations fall under three headings—equity, sovereignty, and democratic accountability and oversight.

First, on equity, most importantly, ArriveCAN should always have been a voluntary app. It never should have been mandatory. The first proposal here is to implement mandatory redundancy in our digital public service delivery. What this means is that if there is a digital way to access a public service, there always, including in emergencies, needs to be a non-digital mode as well, one that is properly staffed and delivers just as high quality and experience.

Two very telling things happened over the course of ArriveCAN that illustrate why we need this kind of policy as a gating mechanism to force equity in public service delivery.

First, the government roundly ignored the federal, provincial and territorial privacy commissioners who stated clearly that technology used during the pandemic must be voluntary in order not to destroy public trust. To quote from the 2020 joint statement by federal, provincial and territorial privacy commissioners entitled “Supporting public health, building public trust”:

> Consent and trust: The use of apps must be voluntary. This will be indispensable to building public trust. Trust will also require that governments demonstrate a high level of transparency and accountability.

Second, the public service should have had a deep and clear knowledge of the access and digital literacy issues, the discomfort and the fear that mandating this technology created for people in this country. This is about public service ethics. Yes, we were operating under emergency powers. If anything, this should have increased the care taken to support comfortable human experiences. Instead, the moment was used to accelerate an underlying desire to modernize the border.

Our work of democracy is easing access to each other's care. The mandatory nature of this app did the opposite. It created barriers. It devalued the work and possibility of the public service.

My second proposal is on sovereignty: Do not deliver public services through apps and app stores, full stop. We should not be building the delivery of public services with and through digital infrastructure that we don't own or control. This should be a non-starter.

The app stores are for consumer products. They are not for government service delivery. There is also a significant issue with moving the work done by the public service away from physical interactions and into private devices done in private places.

One of the problems with honing in on procurement is that we talk about purchasing. We skip over what it would mean to build our digital infrastructure, which is a conversation we need to have more of.

Finally, on democratic accountability and oversight, a third proposal is to create an independent public advisory board to oversee ArriveCAN's ongoing development and use. This will help address transparency problems, open the code, explain where the data goes and how it's used, and engage with communities on changes and updates to the app. The app's development is funded into next fall, so there's lots of time to set up an improved oversight mechanism.

In closing, the development, design, launch and implementation of ArriveCAN was rife with digital governance issues and errors. We can do better in the future, but only if we understand, acknowledge, and accept the harm caused by ArriveCAN and the lack of defensible public health rationale to do so.

Thank you. I'm happy to discuss any and all of this further.

● (1535)

The Chair: Thank you, Ms. Wylie. I appreciate your staying to time because that will give us a lot more opportunity for questions.

Mr. Malone, you have five minutes, sir.

The floor is yours.

Mr. Matt Malone (Assistant Professor, Thompson Rivers University, As an Individual): Thank you, Mr. Chair.

My name is Matt Malone. I am an assistant professor at Thompson Rivers University in the faculty of law. I am attending the hearing today in a personal capacity, representing only my own views.

[*Translation*]

I'd like to thank the committee for this unexpected invitation and opportunity to discuss my privacy concerns regarding the ArriveCAN application.

After my opening remarks, I would be glad to answer the committee members' questions.

● (1540)

[*English*]

First, I would like to talk about how the government failed to take reasonable steps to ensure that personal information collected and retained by the app was kept safe. Unquestionably, the worst example of this was the glitch that sent 10,200 people who had correctly used the app faulty quarantine orders. The government's response to and transparency about the glitch were appalling. Some affected users were not notified that they were victims of the glitch for 12 days. During those 12 days, the ArriveCAN privacy notice stated that disobeying a quarantine order issued by the app was punishable by a fine of up to $750,000, or six months in jail.

When I wrote about this issue in the Globe and Mail in August, I received numerous harrowing stories from Canadians. This correspondence made it very clear that many elderly and rural Canadians in particular were seriously affected. In my own experience, when I requested the personal information about me, collected by CBSA through the app, it was not forthcoming from CBSA for four months. When I finally received it, there were many errors in my personal information.

The foregoing suggests that the government failed to take reasonable steps to ensure that the personal information it collected was both adequately safeguarded as well as accurate, up to date, and complete, as required by section 6 of the Privacy Act.

Second, I want to talk about secrecy. CBSA has not been forthcoming with Canadians or Parliament, including this committee. On November 14, 2022, the CBSA president told the government operations and estimates committee that the CBSA spent 4% of its budget on ArriveCAN for security. But it has produced almost no records speaking to those efforts.

The work of the primary contractors involved in building ArriveCAN also raises serious concerns. Based on my review of previous access to information requests, extensive correspondence between GC Strategies' managing partner, Kristian Firth, and Canada's chief technology officer, Marc Brouillard, shows that GC Strategies appears to operate more as an unregistered lobbyist than a primary contractor. As a primary contractor, it appears that the only real service they offer is secrecy, by subcontracting work through contracts that are shielded from disclosure as proprietary information. This is a deeply unsettling way to deliver government services that involve the mandatory collection and retention of Canadians' personal information.

Third, I want to talk about the justification for the app. I have noted in my public and academic writings that the mandatory use of ArriveCAN did not meet the threshold under the Quarantine Act for emergency measures. Moreover, the government's rationale for the app kept changing. This became most obvious following the introduction of the "advance CBSA declaration", an optional feature that was inserted into the mandatory architecture of the ArriveCAN app. When the advance CBSA declaration was unveiled, it was done so hastily that the government did not include a privacy notice as required under subsection 5(2) of the Privacy Act. I believe this also likely implicated sections 4 and 7 of the Privacy Act.

Fourth, I want to talk about the government's disregard for existing oversight measures when it introduced ArriveCAN. With ArriveCAN, many of these measures were simply ignored entirely.

[*Translation*]

It is crucial to point out that the government disregarded key measures in a number of acts and directives—the Directive on Automated Decision-Making, for one.

[*English*]

Fifth, I believe this episode underscores the need for urgent reform in the access to information system. We need robust access to information that sheds light on the work of quasi-lobbyists like GC Strategies. Using such entities to deliver services that are making decisions about Canadians and are subject to neither disclosure nor review is concerning in the context of mandatory collection and retention of Canadians' personal information.

Ironically, GC Strategies itself once even pitched to the Treasury Board Secretariat using subcontractors to reform the access to information system's search function itself. The existing system needs more funding and more disclosure. Many of my own requests have been egregiously delayed. Some have been simply ignored. I'm happy to discuss those.

Finally, to echo the comments of my colleague Bianca Wylie, for whom I have great respect, I want to emphasize that the government should never have deviated from its own promises early in the pandemic that it would introduce health apps only on a voluntary basis. This was echoed and supported by a joint statement of all privacy commissioners, who came together to say the same.

I believe public trust is essential in driving successful technology adoption, and I believe this kind of trust cannot be mandated.

[*Translation*]

Again, I'd like to thank the committee for inviting me.

[*English*]

The Chair: Thank you, Mr. Malone.

We'll start with our questions. The first round will be six minutes.

We'll start with Mr. Barrett.

Mr. Michael Barrett (Leeds—Grenville—Thousand Islands and Rideau Lakes, CPC): Thank you, Chair, and thanks, Ms. Wylie and Mr. Malone, for joining us here today.

I will start with you, if I can, Ms. Wylie.

What are the risks that happen when security clearances are waived for some subcontractors who would be working on an app that deals with Canadians' biometric data, personal health data, and passport information? What are the risks to their personal privacy rights when something like that occurs?

Ms. Bianca Wylie: They are numerous, in terms of the fact that when you don't know how data can move and how it can evolve, if you lose control of it and you're allowing people to use it outside of the construct within which people thought it was collected, you can have problems.

One thing that's important to know is that data is so easily replicated and then adapted and moved that losing control over how it's managed or used is a serious risk and creates significant liability. Should there be reasons to have exceptions to these rules? One would hope that those would be made clear and would make sense. The rules are there for a reason. That's a question of process. If there's an exception, why?

● (1545)

Mr. Michael Barrett: Right. All of our public service employees already have the requisite clearances. Keeping a program like this in-house and developing it over time would eliminate that particular risk.

You talked about some of the examples on how data can move and how it can be later utilized. Can you give us a brief example of one of those risks?

Ms. Bianca Wylie: For any kind of data breach, it is difficult to follow where the data goes and how it's been used. We're seeing how numerous they are. Really, this is why you want to minimize data collection in the first place, because once things have a breach it's very difficult to follow, continue and understand. This is one of those situations where you can't put the toothpaste back in the tube.

Mr. Michael Barrett: Right.

You talked about public trust. What impact does mandating the use of this technology have on public trust?

Ms. Bianca Wylie: Thanks for asking, because I think that was the most significant outcome here. Without confidence in how the government is using data, the public can't trust it.

In this instance, the fact that this was mandated and there was for sure a lack of clarity from the government to the people as to how this data was being used, beyond the idea that we're in a pandemic where there's a crisis and therefore you must do X.... What happens when there are already issues with trust is that this accelerates the distrust. This was so unnecessary, because some people like this app, and if they like it and they feel comfortable using it and they can consent, perfect. If someone is not that person, they need a great path to access public service too. The failure to create that path just really inflamed this trust and it was a very difficult point in time.

We can see it's a completely unnecessary loss of trust and it happened. As it was happening, it was shocking to me that—I don't know how much people here saw—there were concerns about how this data could or couldn't be used because it wasn't clear, and this accelerated and was fomenting distrust. That's the word to use here.

The obvious antidote is that you build alternatives for people. This lack of investment to make sure people were comfortable.... To Matt's point earlier, if you want to get into good digital service delivery, you're going to get there by building trust and bringing people along with you. You don't force it; you open it up. If you like the option, you use it and then you continue along.

Mr. Michael Barrett: Thanks very much.

I'll turn to you, Mr. Malone, with respect to the governance issues that you see with the execution, but also with the development of the app.

Mr. Matt Malone: The government has in place many policies and directives that should guide the development, construction and deployment of an app like ArriveCAN. What's boggling in this instance is that it essentially threw all of these well-developed policies out the window. For example, the directive on automated decision-making states that there should be an algorithmic impact assessment done at the time artificial intelligence will be deployed, so when that is constructed at the outset of the program, that will do that. That never occurred.

The only algorithmic impact assessment that is available, to my knowledge, is one that was done a year and a half after ArriveCAN was introduced. The policy, the directive, says that the assessment should also occur whenever the app is significantly updated. That occurred at many instances, but rather than adhering to its own policies, the government simply unveiled the developments in the app store. That's what got the government into trouble when it introduced an advance CBSA declaration into the iOS version of the app, because it was an update in June that caused the glitch.

Mr. Michael Barrett: To be clear, with respect to the assessment of potential impacts, you're talking about the potential impacts that it would have on the user, like mandatory quarantine or, effectively, house arrest and facing possible jail time or substantial monetary fines.

Is that the type of impact?

● (1550)

Mr. Matt Malone: No, not precisely—

The Chair: Give a very short answer, please, Mr. Malone.

Mr. Matt Malone: The directive has risk mitigation items, and they're slightly different from that.

The Chair: Thank you, Mr. Barrett.

Next we'll go for six minutes to Mr. Fergus.

[*Translation*]

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

Thank you to both witnesses for being here.

Ms. Wylie, I was fascinated by your remarks, so I have a series of questions based on what you've said here and in posts in which you express your views on the subject.

First of all, you raised concerns about the security of people's personal information. Are you aware that the Public Health Agency of Canada, PHAC, had asked the Privacy Commissioner of Canada to evaluate the safeguards relating to Canadians' data in the ArriveCAN app?

[*English*]

Ms. Bianca Wylie: Yes.

[*Translation*]

Hon. Greg Fergus: Are you aware that the commissioner had done an evaluation of the ArriveCAN app and found no major concerns?

[*English*]

Ms. Bianca Wylie: I know what the Privacy Commissioner shared back. However, the reason we both raised.... The privacy commissioners all had the concern with the app being mandatory, rather than voluntary. That came from the Privacy Commissioner, because there's no one else in the government who has a mandate to look at the application of the technology.

In this situation, when we're talking about trust and people's concerns, we need to break out of the privacy paradigm and into the question of appropriate use and ethics.

[*Translation*]

Hon. Greg Fergus: What you are talking about is a political issue, rather than a specific directive or failure by the government to protect Canadians' privacy in the face of a public health threat to Canadians and Canada.

[*English*]

Ms. Bianca Wylie: To me, this is not a political topic at all. We can bring in two facets of the existing government, open government.

What was the public health impact of ArriveCAN? This has not been communicated clearly to the public.

In terms of decision-making about the use of technology, I'd like to share with everyone here that there was a major cultural deference to the Public Health Agency of Canada, which makes a lot of sense in a pandemic. However, deference to the Public Health Agency of Canada on the use of technology does not make any sense. This is not something where the implications of applying technology and all of its related infrastructures that are upstream of both PHAC and CBSA...these are totally different issues that don't sit neatly in the realm of privacy.

This second piece here is important, as well, which is that we understand why the Public Health Agency of Canada—nothing in the Quarantine Act said that we had to have an app, nor a mandatory app—had the authority to exert that decision, when it was against what all of the privacy commissioners recommended for public trust. If there was a good reason, back to open government, it should have been communicated, but it wasn't.

[*Translation*]

Hon. Greg Fergus: In your opening remarks, you said no public service should be delivered through an app. Doesn't that fly in the face of the modern age we live in, when people have a growing appetite for easy-to-use services? During the pandemic, for example, the federal government created an online service to deliver the Canada emergency response benefit, financial support for people in need who had lost their jobs.

The trend is towards delivering user-friendly services to people while protecting their privacy.

● (1555)

[*English*]

Ms. Bianca Wylie: We need to make a distinction here between the Internet and the web. You can have technology that is designed for the Internet and for mobile devices that is not apps that are available through the app store.

When Google and Apple and their iOS systems become implicated in the delivery of our public services and we're not in charge of how Google and Apple develop their mobile operating systems, we are creating a dependency in our technical infrastructure that is a major liability.

We can have modern technology. It doesn't have to live in the apps.

The Chair: Mr. Fergus, I'm sorry. We're 45 seconds over.

If you want to pick that up later, I would encourage you to do that.

[*Translation*]

You have six minutes, Mr. Villemure. Go ahead.

Mr. René Villemure: Thank you, Mr. Chair.

Mr. Malone, you've worked for many tech companies.

Mr. Matt Malone: No, I was a lawyer in California.

Mr. René Villemure: What type of law did you practise?

Mr. Matt Malone: I worked for clients in the tech and digital sector.

Mr. René Villemure: All right.

You said in your opening remarks that the government had not taken any reasonable steps to protect people's personal information. Can you give me an example of a reasonable step the government should have taken?

[*English*]

Mr. Matt Malone: Yes, I think the ultimate recommendation that this would come down to if we were in an alternative world would simply be to follow the government's own recommendations and the directives that it has in place, like the directive on automated decision-making, for example. That directive encourages source code in applications to be rendered public by default. In this case, that did not happen—distinct from other health apps designed to prevent the transmission of COVID-19.

Additionally, that directive also sets out that there should be meaningful explanations of how the artificial intelligence such an app might be using is being used to make decisions affecting Canadians. In this case, it's very difficult to get those explanations; we never got them. A large part of that was because the subcontracts from the primary contractors that the CBSA and PHAC used were essentially trade secrets and confidential information. Before the government operations and estimate committee on November 14, a representative from PSPC said very clearly that this information is information that is treated as proprietary, which was very concerning to me.

[*Translation*]

Mr. René Villemure: You don't think it's confidential information.

[*English*]

Mr. Matt Malone: No, I think that there should be maximum transparency and accountability, as intended in the Access to Information Act. The manual for that act says very clearly that the underlying contracts with businesses that are doing business with the Government of Canada should be open by default. There should be no presumption of confidentiality.

I don't understand why the presumption of confidentiality exists, when it's only a subcontract. I think that all of those subcontracts should be rendered public. I think it's in the public interest to know them, all the more so because of the fact that the largest of the contracts was granted in a non-competitive bid.

[*Translation*]

The Chair: Pardon me, Mr. Villemure. I'm stopping the clock. That was the second time the interpreter couldn't understand your question. Can you please speak slower?

Mr. René Villemure: Of course. Thank you, Mr. Chair.

Please carry on, Mr. Malone.

● (1600)

[*English*]

Mr. Matt Malone: Essentially, I think the problem is that...subcontracts should be rendered open by default.

[*Translation*]

Mr. René Villemure: You mentioned GC Strategies and the many subcontractors that were used.

Do you think having so many people involved can indirectly influence public policy?

[*English*]

Mr. Matt Malone: I'm not sure I would have enough knowledge to answer that question, quite honestly.

[*Translation*]

Mr. René Villemure: All right. Thank you.

Ms. Wylie, you talked a lot about trust and the risk of eroding that trust.

You contacted the Privacy Commissioner, and he gave you his response. Are you satisfied with that response?

[*English*]

Ms. Bianca Wylie: No.

[*Translation*]

Mr. René Villemure: Why not?

[*English*]

Ms. Bianca Wylie: It's not enough. One, we look at our technology in the frame of privacy. We're downstream from questions such as these. Should this exist? Should we build it? Should we buy it? If we buy it, how are we going to build it, how are we going to maintain it, and how are we going to sunset it?

There are numerous issues that happen upstream of what the commissioner has a mandate to oversee. So there's a lot that doesn't land there, and that to me is an ongoing concern.

[*Translation*]

Mr. René Villemure: Would you say that the commissioner focused on how the ArriveCAN app worked, as opposed to why it existed?

[*English*]

Ms. Bianca Wylie: Once they made their statement in 2020, we saw the advice: Don't make it mandatory; make it voluntary. From that point forward, it appeared as though they were supporting the implementation, and I didn't see much resistance.

[*Translation*]

Mr. René Villemure: I see.

I agree with you about the damage done to public trust. What can we do now to restore that trust?

[*English*]

Ms. Bianca Wylie: Do you mean with ArriveCAN specifically?

[*Translation*]

Mr. René Villemure: Yes.

[*English*]

Ms. Bianca Wylie: With the setting up of a public oversight body, which we had, you could almost immediately replicate what was done for the COVID-19 Alert app. You bring in a group of people, you have meetings, they can help communicate issues back to government, and you can have an audit of the app and open the code. There are numerous things we could replicate from the lessons of the COVID-19 Alert app, so that's an easy one.

I think the other thing we need to do is be clear about what the pandemic impact was of ArriveCAN, because somehow we just keep getting this: “It's an emergency, and we have to do it.” However, what was the public health rationale, and what was the outcome of ArriveCAN on the pandemic?

[*Translation*]

Mr. René Villemure: The government didn't learn any lessons from the COVID Alert app before developing the ArriveCAN app. What is it going to take for the government to learn from its mistakes?

[*English*]

Ms. Bianca Wylie: I have no idea, because this keeps happening over and over again. I want to make clear that this notion of modernizing—by just thinking let's accelerate, let's modernize and let's be somehow in the future—has infected the public service and the culture of senior management.

I need to disclose that I saw people celebrating the number of downloads of this app in the middle of a public health crisis, in comparison with apps that have nothing to do with the public service. So the incentives inside the government need to be explored, because there are problems there within the public service.

[*Translation*]

Mr. René Villemure: [*Inaudible—Editor*] certainly reflect instead of react?

The Chair: Please repeat your question, Mr. Villemure. There was an issue with the microphones.

Mr. René Villemure: All right.

Should the government reflect instead of react?

[*English*]

Ms. Bianca Wylie: If we want to look at how we want to modernize the government and the use of technology—and I understand that we want efficiencies—we cannot put efficiency over the experience of people who are receiving services from the Government of Canada. Sometimes people will need an inefficient approach, and what we have to figure out here is the balance. We cannot go all in on tech. We have to make sure we're building redundancies. Do people remember when we had the Internet outage? The app wasn't working at the airport for a day in Pearson, and of course we had redundancy.

The public service has to be built on redundancy. It can't just be all one way. We can do great technology, and we can build it, but we have to be intentional about how. We have to support every single person who needs to access the public service in an equitable way.

● (1605)

The Chair: Thank you.

[*Translation*]

Thank you, Mr. Villemure.

[*English*]

Mr. Green, you have the floor for probably a little more than six minutes.

Go ahead, sir.

Mr. Matthew Green (Hamilton Centre, NDP): Thank you very much. I'm happy to take my six minutes.

I want to welcome the guests. This is a very important investigation into, hopefully, some of the ways we can improve upon privacy and the use of technology.

I want to allow Ms. Wylie to expand on two notions to begin with. The first is this culture that she commented on. I'm wondering if Ms. Wylie could expand on some of her observations—in her opinion and in her own words—and how she feels the bureaucratic culture might be counterintuitive to being able to provide good and effective digital products to people who respect civil liberties and privacy.

Ms. Bianca Wylie: Thank you for the opportunity to expand on this.

As I understand, within the public service, at senior levels, if someone receives some political enthusiasm for an app or for a technology, for something that's going to be innovative or modern, there is very little space to push back and to say, “You know what? This approach might not make sense”, or to ask where this is coming from or from whom. Which firm or which person has an interest?

I need to return to the app stores for a moment, because if we need to understand anything.... At this point in time, in 2022, companies like Google and Apple want to be living in the infrastructure that we use in our public services across the board. They have no subject matter expertise to be involved in public health or border services.

The point here is that if we don't begin to understand the need to develop both good and future-oriented technology in the public service, there has to be room for senior management to say, “I hear what you want to do with technology, but this is actually a bad idea. Here are the reasons why.”

Mr. Matthew Green: You've picked up on an important point.

I'm getting feedback, Mr. Chair. I think somebody in the room might have a mike on.

The Chair: I think Ms. Wylie had her mike on with the earpiece. Maybe that had something to do with it.

Is that better, Matt?

Mr. Matthew Green: It is much better. Thank you.

I apologize.

I wanted to reflect on this notion that we have, perhaps, a culture that would reward corporate, capitalist metrics—i.e., reference downloads—versus the user experience and applicability for public use and public consumption, and ultimately the public benefit.

Is that a fair comment? Perhaps we've adopted too much of this kind of corporatization of public services in order to internally advance some careers and some pet projects.

Ms. Bianca Wylie: Yes, definitely.

Mr. Matthew Green: You talked about the inequities that making a mandatory public service digital creates. Can you describe what some of those inequities might be?

Ms. Bianca Wylie: First of all, we know that not everybody has access to mobile devices or computers. However, far more important than that piece of it, which is known, is the digital literacy to use these things in a way to protect ourselves. There's an inequity there.

An interesting point about ArriveCAN is that, whether people are handing you information on a form or through an app, it's all heading up into an infrastructure and none of us know what it is. We don't know what's going on. If we can't start to explain that to each other—and this is why open government matters—you're not going to get the buy-in from people to use these things.

Mr. Matthew Green: I'm not trying to be reductionist here, but can you define “open government”? Part of the challenge I have is that I feel like we get into these bureaucratic spaces and we use buzzwords all the time. We had a government that said they were going to be open by default, they were going to be the most transparent government and they were going to provide open government.

Can you define, briefly, what that might look like?

● (1610)

Ms. Bianca Wylie: There's open data, there's open science and there's open information. I believe these are the three circles of how this space is defined.

What's really important about open government—and I'm bringing you this from being a facilitator running public meetings—is that people may not like the decisions you make, but if you explain what you're doing, you can get to a good place from a democratic perspective.

To bring this all the way back to your question of what the inequities look like, it's not just, "Do I have a phone or not?" or "Am I comfortable or not?" This second piece, "Am I comfortable or not?".... People were contacting me, much like Matt mentioned. They were scared. They didn't want to travel. They didn't know what they just did. They used an app. They weren't even sure what just happened.

That doesn't get measured in any metrics. That metric doesn't exist. You have these missing pieces of information about how this impacted people. We have, between me and Matt—

Mr. Matthew Green: I'm not sure how much time I have left, so please forgive me.

The Chair: You have about 30 seconds, Matt.

Mr. Matthew Green: There's a really important piece that you can answer in a very short way, and it ultimately comes down to this: In your opinion, should ArriveCAN be audited by the Privacy Commissioner?

Ms. Bianca Wylie: Yes.

Mr. Matthew Green: Thank you.

Thank you very much, Mr. Chair.

The Chair: Thank you, Mr. Green.

[*Translation*]

We will now begin the second round.

Go ahead, Mr. Gourde. You have five minutes.

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

Thank you to the two witnesses for being here today.

Mr. Malone and Ms. Wylie, can you give us some situations where, upon arriving in Canada, Canadians were adversely affected by the ArriveCAN app?

[*English*]

Mr. Matt Malone: Yes, I had my inbox flooded with stories after I wrote my Globe and Mail piece on August 8.

There was an individual in Montreal whom I spoke with on the phone who was quite distraught about his experience trying to get to Vermont for family and for health reasons. There was an individual in rural Saskatchewan who contacted me and said he and his wife did not own a cellphone, and he was reaching out to me from a public library, where he had been trying to print his ArriveCAN.

I can imagine Bianca has stories as well.

Ms. Bianca Wylie: Yes, I have many.

There's an op-ed written by a Canadian in a publication called rabble.ca. Beyond getting the glitch notification, they had a hard time getting an answer from the government about whether there was a glitch or not. They were told on the phone, "No, it's just a glitch", but they were unable to get anything in writing or any confirmation.

I think if we look at the thousands of people who were impacted just on the glitch level, and then the other thousands of people—probably more than that—who were scared to travel or had an uncomfortable experience, we're into very large numbers here with negative consequences for people using this app.

[*Translation*]

Mr. Jacques Gourde: Let's say Canadians filed a class action because of the ArriveCAN app. A number of companies were subcontracted to work on the app, so who would be responsible for the fiasco?

[*English*]

Mr. Matt Malone: I would say that the committee itself has responsibility over certain aspects of the story, and I would turn it a little bit to you.

For example, GC Strategies operates essentially as a quasi-lobbyist. I've put in access to information requests to obtain records of the correspondence and communication that those figures had with figures within TBS and other sectors that were responsible for contracting. It's not entirely clear to me why they were not registered as lobbyists when that is essentially the work they were doing.

In addition to that piece, I would say that the access to information aspect of this story is incredibly important. I have outstanding access to information requests that would be directly relevant to the questions the committee is exploring right now.

For example, in July, I put in a request for assessments of privacy, cybersecurity and data breach risks of the ArriveCAN app, including but not limited to studies, reviews, explanations, audits, manuals, bug reports, validation studies and others concerning the security of the app that the CBSA conducted or that third parties conducted for the CBSA.

The CBSA responded by giving me a 90-day extension, which has subsequently elapsed, and they have simply not responded to my request, which is a violation of the Access to Information Act. That seems directly relevant to the scope of the work of this particular meeting.

● (1615)

Ms. Bianca Wylie: I don't have much to add in terms of the responsibility here. I would consider what precedent there is. I think, at the end of the day, this lands with the government as a whole. I'd have to understand any other case.... When there was a digital product, who was at the end of the line from a liability perspective?

[*Translation*]

Mr. Jacques Gourde: ArriveCAN was said to cost a total of $54 million. Might the contractor and subcontractors have left themselves a considerable buffer within that budget to deal with potential lawsuits?

Maybe that's one reason why the app was developed rather quickly. Other experts say the price tag was pretty hefty for an app that wasn't all that complicated to develop.

[*English*]

Ms. Bianca Wylie: When a product is developed, there's a stage called requirements, writing and gathering. In terms of the time it would take to work between the government and the contractors, that's different from someone saying, this should be fast because I handed you what to build. I think there is a relevant process time in that number.

In terms of the rationale for the cost, without seeing how this went down, I couldn't speak to it. But I want us to remember that what we don't get when we fail to invest in a public service is reuse. If we're spending this much money, we should be investing into the capacity and code with conditions that we can reuse as the federal government. This to me is a bad spending decision regardless.

The Chair: Thank you, Ms. Wylie.

Next we have Ms. Hepfner for five minutes.

Ms. Lisa Hepfner (Hamilton Mountain, Lib.): Thank you, Chair.

I would like to start off my questions through you to Mr. Malone.

I heard you talk about breaches to the app, but then you went on to describe faulty quarantine notices that went out. It wasn't that it was a breach of data or personal information; it was 10,000 false quarantines that went out to people, which is about 0.03% of the 30 million times that it was used.

I'm wondering if you have any evidence of data breaches or personal information being leaked from this app.

Mr. Matt Malone: There is one outstanding access to information request, which I believe dates from the summer of 2021, which is viewable—

Ms. Lisa Hepfner: You have a request out but you have no information at this point.

Mr. Matt Malone: No, no, there's one request that is not mine that is already processed, which confirmed that as of the summer of 2021 there had been no breaches. Then I put in a request for confirmation from the CBSA's media unit in early September, and they also confirmed that there were no data breaches.

That's separate from my outstanding request to know more about the studies that were done to prevent data breaches. So far, I've heard that there have been no breaches of the app as of September 1, 2022. That is separate from the glitch that sent those erroneous quarantine orders.

Ms. Lisa Hepfner: Thank you. That's helpful.

Ms. Wylie, I was listening to you talk about how ArriveCAN is sort of closed code. You've been advocating that it be open code so that people can understand it better. To quote Mr. Barrett, at the OGGO study that revolved around these same sorts of things, the app contains biometric, personal and health information of more than eight million people who downloaded the app. Mr. Barrett was concerned about hypothetical bad actors who could build in a backdoor access to this information in the future. He said, "There are a lot of ways that foreign state actors can test our systems and our processes, and this looks like a great opportunity for them to do that."

Do you agree, based on this sensitive information, that this app should have been developed with the highest degree of sensitivity and the most constraints around our personal information?

Ms. Bianca Wylie: Making the code base for the app closed doesn't create the security that I think you're suggesting. Of course, it should be well developed, but it could be well developed, and with an eye to what is being collected and used, but still be open-source code. The mechanics, the underlying code, the architectures, how it works, there's no problem with that being open and also with it serving the purpose that it served.

● (1620)

Ms. Lisa Hepfner: Okay. You don't see any privacy concerns with that.

This study focuses specifically on the cost associated with ArriveCAN and the handling of personal information. You talked about how there should have been, from the beginning, redundancies so that people didn't have to use the app. But I'm wondering if you took into account how much it would have cost to have all those redundancies put in from the beginning.

Ms. Bianca Wylie: Yes, I definitely did. I don't think you can put a price on trust. I think with the damage that this app did to public trust you could have tripled what was spent on ArriveCAN to make sure that kiosks were updated or that they were staffed.

Ms. Lisa Hepfner: Did you crunch the numbers?

Ms. Bianca Wylie: No. But however much it would cost not to have lost this trust would have been a worthwhile investment.

Ms. Lisa Hepfner: Do you know of any breaches of personal data or privacy that came from using the app?

Ms. Bianca Wylie: I do not know of any, no.

Ms. Lisa Hepfner: In your expertise, what challenges would exist to ensure the integrity and safety of the data that people provide to a company or in this case the government?

Ms. Bianca Wylie: The best principle is always minimization. This is why I repeatedly ask what the public health rationale was for ArriveCAN to be developed as an app. I don't understand what the public health rationale was for this act.

Ms. Lisa Hepfner: That wasn't my question.

Can you explain to us, from your expertise, how to ensure the integrity and safety of the data that people provide?

Ms. Bianca Wylie: I'm sorry. I didn't make a clear enough connection.

The first step is data minimization. You don't collect it if you don't need it.

This becomes the question in terms of what was collected and how it was used by the Public Health Agency of Canada. I don't know, but, if it was necessary to have that information, then you get into all your basics in terms of storage and who has access, as Matt has mentioned. We have good policies for how to design secure architecture.

I'll keep going back to the first point, which is that you don't want to hold data unless you really have to.

Ms. Lisa Hepfner: Thank you.

I think my time is up.

The Chair: Thank you.

[*Translation*]

You have two and a half minutes, Mr. Villemure.

Mr. René Villemure: Thank you, Mr. Chair.

Ms. Wylie, do you think the general public understands the issues associated with the use of an app like ArriveCAN?

[*English*]

Ms. Bianca Wylie: Absolutely not.

[*Translation*]

Mr. René Villemure: Do you think it's appropriate to teach people about digital literacy, since these kinds of issues can be hard to understand?

[*English*]

Ms. Bianca Wylie: Absolutely, and when I say that, that includes me, because I don't even know where this information goes once it moves into government infrastructure and architecture.

I want to say that this government had people uploading their passport information on airport Wi-Fi. It's not just what the app is and what the code is; it's what the habits are and what the use protocols are that you're encouraging people to follow when you develop and implement an application such as this. If this government is following these approaches and is also in charge of digital literacy, I would still be concerned.

[*Translation*]

Mr. René Villemure: It's definitely concerning. It certainly does not inspire confidence.

You posted that "the extension of the administrative state through modernization and digital transformation is made to seem mundane but its current and future impacts are anything but."

Can you elaborate on that? I have about a minute left.

[*English*]

Ms. Bianca Wylie: What I'd like people in this room to know is that modernizing government is still fairly novel. There's a lot of excitement about things that are novel. We have not reckoned with the consequences about redress, how we have access to justice when things go wrong with digital public service delivery. A lot of people seem to get caught up in this enthusiasm for modernization, but we still have a whole bunch of stuff we haven't even reckoned with in terms of issues and access to justice.

I would really like us to think about reducing the inherent enthusiasm for putting technology on top of and through everything in ways that are not thoughtful.

● (1625)

[*Translation*]

Mr. René Villemure: Thank you.

In a few seconds, Mr. Malone, can you tell me whether you think the public understands what using an app like ArriveCAN means?

[*English*]

Mr. Matt Malone: I don't think they know, but I think they can feel concern around it, and I think that is what's palpable in the public discourse.

[*Translation*]

Mr. René Villemure: Can that erode public trust?

[*English*]

Mr. Matt Malone: Absolutely. I think the fact that the app delivered erroneous orders to people who used it correctly is detrimental to building trust.

[*Translation*]

Mr. René Villemure: Thank you very much.

[*English*]

The Chair: Thank you, Mr. Villemure.

Mr. Green, you have two and a half minutes, please.

Mr. Matthew Green: Professor Malone, do you also agree that we should have an audit of the ArriveCAN app through the Privacy Commissioner?

Mr. Matt Malone: Yes. The Office of the Privacy Commissioner, to my understanding, currently has at least two complaints before it regarding ArriveCAN. One of them is my complaint.

The Privacy Commissioner has also stated quite clearly that there are no data-sharing agreements in place for how the data is being transmitted by the subcontractors that are hidden behind those contracts.

Mr. Matthew Green: Professor Malone, what's the impact of that?

Mr. Matt Malone: What's the impact of not having data-sharing agreements in place? It doesn't govern how the data will be used. Essentially, it obviates the consent that users would be able to give as to how their data would be used, which is a very important provision within the Privacy Act itself.

We have problems here with whether the data was being kept accurately in a manner that was complete but also up to date. When I requested my own data, saw my data, and saw how the algorithms were interpreting my passport, reading my name, spelling my name and scrambling my phone number incorrectly, it was very clear to me that this app was shoddily constructed.

Not only do we have a problem with the accuracy of the data but also in terms of how the data is being shared by these entities whose names are all we know about them. That is a big problem when it comes to informed consent as required in the Privacy Act.

Mr. Matthew Green: Carrying on from that, in "Lessons from ArriveCAN: Access to Information and Justice during a Glitch", you wrote that the government "failed to place the data collected from ArriveCAN into a Personal Information Bank, despite the requirements of the Privacy Act."

Can you describe the potential consequences of this failure?

Mr. Matt Malone: I essentially asked the CBSA's media arm for information about what personal information bank, as required in the Privacy Act, they'd been placed into. The CBSA media arm refused to provide any answer whatsoever, which led me to believe that they simply had not done it.

As for this data, which had been collected and retained for a minimum of two years with no expiry, as the privacy notice for ArriveCAN itself stated, who knew where it was going? Who knows where it is now?

Mr. Matthew Green: Lastly, I just want to ask both witnesses who are present here today if they would consider providing in written remarks any recommendations that they might have relating to changes that should be made in the Privacy Act to perhaps prevent this from happening again.

Thank you.

The Chair: Thank you, Mr. Green. We'll take that as a request from Mr. Green for both of our witnesses.

We have Mr. Barrett for two and a half minutes, followed by Ms. Khalid, and that will be the end of the panel.

Thank you.

Mr. Michael Barrett: Thanks, Chair.

I just want to be really clear. This is an app that erroneously caused 10,000 people to have their civil liberties suspended and be ordered under house arrest, and a breach of that order was warned against with threat of jail time or fine.

There's been a characterization that this is a small number in the context of the total number of users of the app. This is offensive. This is 10,000 people who followed all of the rules. They broke no laws, and they were ordered not to leave their homes or they would be put in jail. They were ordered by an app that they downloaded in the app store.

There was no way for them to redress that grievance. There was nothing for them to do. When they called my office, as they called many other folks, we tried to intervene for them, and it was about day 16 or 17 of their 14-day quarantine before they were able to have demonstration that they were, in fact, still free.

It's so important that we highlight that.

Mr. Malone, you mentioned GC Strategies a couple of times. This is a company that has two employees. It took in $9 million. It did no tech work on this app that was entirely technological in nature, handling sensitive data. To be clear, this two-person company, when they did appear at a parliamentary committee, couldn't even say which of the two of them answered the telephone when the government called to award them a $9-million contract that they wouldn't have to do any tech work on. We don't know who their subcontractors are. There is a lack of transparency.

I've used a lot of time here.

You talked about securing access to information laws and potentially lobbying rules. Are you able to expand on that a bit with the remaining time?

● (1630)

Mr. Matt Malone: What I've seen from the access to information request I referenced, which is 2018-00247, GC Strategies had very regular contact with the chief technology officer of Canada. There's a reference in an email that they typically touch base once a quarter. I can produce the records for the committee, which are essentially just pitches they would pose as an intermediary company, where a third party technology company would provide services. For example, they pitched a project to the chief technology officer to reform the access to information's search function on the Open Canada website.

As a starting point, I would like to get the correspondence and dates of the calendar meetings between those individuals. I think that's really important. There is a registration function for lobbyists, which I think probably should be the case for entities like this. Within the access to information system, the sort of manual itself, I think there should be clearly enunciated rules that subcontracts in these types of situations should be open.

The Chair: Thank you, Mr. Malone.

Mr. Michael Barrett: Chair, during Mr. Malone's response, he offered documents. Is that something that we can have the clerk collect?

The Chair: We can certainly have the clerk follow up with Mr. Malone on that.

Thank you, Mr. Barrett.

Mr. Michael Barrett: Thank you.

The Chair: Ms. Khalid, you have two and a half minutes, please.

Ms. Iqra Khalid (Mississauga—Erin Mills, Lib.): Thank you, Chair. I appreciate it.

I'll start with Ms. Wylie.

Have you used the ArriveCAN app?

Ms. Bianca Wylie: No, I haven't.

Ms. Iqra Khalid: Mr. Malone, have you used the app?

Mr. Matt Malone: Yes, I've used it five to 10 times.

Ms. Iqra Khalid: Thank you.

Ms. Wylie, in your opening remarks, you gave a couple of recommendations. You said that digital must be complemented with non-digital and that public service should not be delivered through apps or web-based applications.

When it came to the government protecting the personal health data of Canadians, do you think that having electronic apps that processed 30 million submissions would be safer than having paper-based records? What measures do you think would be more protective of paper-based as opposed to digital records?

Ms. Bianca Wylie: This is good, because I get to complete a thought from earlier. Web-based apps, being able to use the Internet to go.... ArriveCAN had three options. You could use it on your computer, just by logging in with an email, or you could use it through Apple or Google operating systems. This version where you work through the web is the one that is the most open. It is the one where the protocols are the most accessible to everybody and where, from a technical design perspective, we have a better shot at doing digital, without the constraints imposed on us by Google and Apple through the app stores.

I'm not saying there should be no digital. What I'm saying is that the web application, mobile design that's responsive to the web, is an option for sure.

To your point, yes, there may be improvements in the fidelity of the data collection, or whatever else, through using these things, but no matter what we do, we can always improve our public services as well to make sure that whatever.... How we improve accuracy for things we receive on forms or at kiosks, or whatever else, those are improvements we need to make concurrently.

I'll stop there.

Ms. Iqra Khalid: Thanks, Mr. Chair.

Those are all the questions I have.

The Chair: Thank you, Ms. Khalid.

On behalf of Canadians, I want to thank both of our witnesses, Mr. Malone and Ms. Wylie, for being here today. I think you provided the committee with some valuable information.

I will remind committee members that we are going to come back and resume with the access to information study.

I'm going to suspend for a few minutes, but before I do, keep in mind that in terms of the microphones, sometimes there is a little bit of a delay, a couple of seconds. When asking questions, be mindful of that. It will help the interpreters.

The meeting is suspended until we get set up for the next half of the meeting.

● (1635)

_____(Pause)_____

● (1635)

[*Translation*]

The Chair: We are now resuming.

[*English*]

Pursuant to Standing Order 108(3)(h) and the motion adopted by the committee on Monday, May 16, 2022, the committee is resuming its study of the access to information and privacy system.

Madam Clerk, this is just to confirm that all of the witnesses have been tested, from a hearing and speaking standpoint.

● (1640)

The Clerk: Yes.

The Chair: Thank you.

I'd like to now call our witnesses for this afternoon.

First of all, we have, as an individual, Mary Francoli, associate dean and director of the Arthur Kroeger College of Public Affairs. As well, we have, as an individual, Mr. Patrick White.

Again, this is about access to information.

Ms. Francoli, the floor is yours. You have five minutes to address the committee.

Thank you.

Prof. Mary Francoli (Director, Arthur Kroeger College of Public Affairs and Associate Dean, Faculty of Public Affairs, Carleton University, As an Individual): Thank you so much for having me.

I want to start today by saying that my own work is on transparency and open government more broadly. Access to information is certainly an important cornerstone, but transparency itself is more extensive. I think that will be useful because the motion that passed to initiate your study refers to the “access to information and privacy system”, not specifically to the Access to Information Act, which is, to me, a little bit more specific.

I don’t want to repeat any of the points made by previous witnesses regarding the Access to Information Act itself. This has to be one of the mostly widely studied pieces of legislation there are, and I think there's been a great deal of agreement, obviously not unanimous, on the problems surrounding the act and what could be done to improve them. I’m happy to speak to that during questions and I’ll reinforce many of the points you’ve already heard.

I thought I would use my opening remarks to draw on my experience as the chair of the Open Government Partnership’s international experts panel and my experience over the last three years with the national security transparency advisory group, or the NSTAG, as we’ve come to be known.

I will start by saying there is no clear or very coordinated transparency strategy in Canada, but I think this committee should note that a lot of activities are taking place—in many cases they are actually quite siloed—that are meant to improve the quantity and quality of information and data disclosure, and to improve transparency and accountability in government. If done well, these things should, theoretically, help to ease pressure on the ATIP system itself.

Canada has submitted five action plans to the Open Government Partnership, which include a range of commitments to improve openness. Some of the 2015 improvements to access to information mentioned by previous witnesses here were the result of commitments included in early plans to the Open Government Partnership. The plans engage a wide range of government departments and agencies and they have helped to release information and data via the creation of mechanisms like the open science and data platform.

Library and Archives has done a lot of interesting transparency work, in spite of the fact that it's been heavily criticized for compliance with the Access to Information Act.

The government has elaborated a national security transparency commitment. The NS-TAG has a role in helping to advance this. We've released three reports to date. The first was kind of to simply say what we heard in our first year. The second looked at building transparency into national security institutions. The third looked at how national security institutions engaged with racialized communities. From what I understand, the government is also working on an open government strategy for the OECD.

For me, a full study of the access to information and privacy system—again, I'm stressing the word "system"—needs to go well beyond the act itself. It needs to include these other activities. It needs to include offices beyond just the Information Commissioner and the Privacy Commissioner.

Just to wrap up, my recommendations would be to have a Government of Canada transparency strategy that brings these sorts of dispersed initiatives together. The structure around the strategy and things like access to information, Library and Archives and systems of information management, all need to be included. That includes looking at things like storage and retrieval and the need for all of these things to be resourced properly.

Emphasis should be put on proactive disclosure and open by default where appropriate. One thing that the NS- TAG has recommended to the national security community is the development of a statement committing to transparency, including what it means to the different security institutions and how it will be measured. This would be helpful across government. Transparency is something that really needs to be baked into the function and culture of government in a way that it currently isn't, including in times of crises.

I will just leave it there. Thank you.

The Chair: Thank you, Ms. Francoli. You're under time, which is always appreciated by the committee.

Patrick White, as an individual, is next.

Sir, you have five minutes to address the committee.

[*Translation*]

Mr. Patrick White (As an Individual): Mr. Chair, members of the committee, thank you for inviting me.

[*English*]

Thank you for the opportunity to contribute to the committee's study on the access to information and privacy, or ATIP, regime.

I am here in my capacity as a citizen of Canada.

Before I begin my remarks, I would like to acknowledge that I make this presentation before the committee today despite fully expecting reprisals or attempts at reprisals from the Canadian Armed Forces and the Department of National Defence.

There is a group of individuals that has been ignored and forgotten during discussions on the ATIP regime. They are the victims and survivors of the abuse of power and sexual misconduct crisis in the Canadian Armed Forces. My evidence today will focus on the interactions of such individuals with the ATIP regime.

To properly understand how problematic the current ATIP regime is, Parliament must understand that the most vulnerable types of CAF members rely on it for access to essential information and records that are needed to make informed decisions about their legal rights and to file fulsome and well-supported complaints. These individuals could be victims of rape or aggravated sexual assault. They could be victims of threats and abuses from reprisals perpetrated by the chain of command. They could be members wrongfully denied employment opportunities or reimbursement for expenses. They could be the 16-year-old who cannot legally drink, smoke or vote, but who received parental consent to join the CAF while completing high school. They could be any combination of the above.

Briefly, I offer some of my credentials and experience. I am a graduate of the Ivey Business School honours business administration program and the McGill University Juris Doctor and Bachelor of Civil Law program. I am an attorney licensed by the Law Society of Ontario, with experience working in corporate law firms in Canada and the United States. I have served Canada for over 13 years as a naval warfare officer in the naval reserve, during which I gained direct familiarity with the ATIP regime. Finally, when it comes to being subjected to sexual misconduct and abuse of power reprisals in the Canadian Armed Forces, I will simply say, me too.

As to the reforms of the system, and to assist victims and survivors, I recommend that the committee consider the following points.

Conduct a stand-alone study of the abuses of the access to information and privacy regime by the Department of National Defence and the Canadian Armed Forces.

Create real penalties for departments that breach ATIP requirements, and provide real remedies for victims, survivors and complainants.

Consider creating a fast-track system under the ATIP regime for identified victims and survivors of misconduct.

Require certain essential pieces of information to be mandatorily disclosed to victims or complainants, unless explicitly waived with written, informed consent.

Require mandatory disclosure of the names of all record-holders who actively handle or are involved in the decision-making process behind a decision that is generated by a complaint.

Pause the time limit to submit complaints, such as grievances, if an information request has been made and disclosure of such information would be relevant in drafting the complaint.

Ensure that records are retained post-retirement, with clear administrative and disciplinary sanctions for those who violate such directives and seek to use retirement to abscond from accountability.

Investigate and implement options for eliminating the “honour system” approach to record disclosure.

Create specific administrative and disciplinary sanctions for those who avoid creating records or who prematurely destroy records.

Identify, at the intake stage, requests for records that the chain of command may resist and require extra scrutiny in the disclosure of such records.

Finally, require mandatory disclosure of search terms used by individual record-holders in response to information requests.

[*Translation*]

Thank you.

[*English*]

I look forward to your questions.

● (1645)

The Chair: Thank you, Mr. White, for your statement.

I'm going to move to the first round of questioning. We're going to start with Mr. Barrett for six minutes.

For the members of the committee, I allowed a little extra time on some of the questions in the earlier panel. I'm going to stick to the timelines tightly because we do have committee business that we have to take care of afterwards.

Mr. Barrett, you have six minutes.

Mr. Michael Barrett: Thank you, Mr. Chair.

Thank you, Ms. Francoli and Mr. White, for joining us.

Mr. White, I want to thank you for your service to our country in the Canadian Forces.

I'm wondering if you could provide the committee with some examples of the difficulties that victims and survivors face in navigating the ATIP system.

● (1650)

Mr. Patrick White: Thank you for the question.

An example that I've personally faced, and I know others have as well, is the amount of information required up front before a request can be processed. As an example, if you're filing an access to information request about records related to a person's misconduct or about an individual who may have assaulted you or harmed you, you're required to provide their service number. The service number is a protected piece of information. To ask a potentially victimized junior member who might not have access to that information to provide it is an immediate barrier, and for them to go to their chain of command to request that information might allow them to be identified as a potential record requester, when the process is designed to allow them to remain anonymous.

Mr. Michael Barrett: The grievance system is the main dispute resolution process for Canadian Armed Forces members. How does the ATIP system interact with the grievance system?

Mr. Patrick White: The problem is that it effectively doesn't, from my experience. The timeline that a member has to file a grievance begins with a 90-day limit from when an action is taken or a decision is made or the member reasonably ought to have known has been made. As I frequently have experienced, the department is extremely tight on timelines when they are applied to victims, but of course not so tight when it comes to responding and meeting their own timelines imposed under legislation.

The circumstances are such that a victim may need information before they make a request. In fact, they may decide not to file a grievance at all if certain information is disclosed relating to a decision or certain information is provided relating to their personal records.

Under no circumstances have I experienced a formal pause on the time limit when someone is looking to file a grievance.

Now, commanders and those who receive the grievances do have the ability to pause and consider grievances beyond that 90-day limit, but it's entirely discretionary. I'm sure when you hear the word “discretionary”, you're right away thinking potential for abuse. Rest assured, there are circumstances that exist that would make that a reality.

Mr. Michael Barrett: How widespread is the problem that you outlined? Is it just the directorate of access to information and privacy within the Department of National Defence? Is that where it stops?

Mr. Patrick White: I wouldn't say so. My experience is.... I am obviously appreciative of the patience and understanding of the officials who work in the directorate of access to information and privacy within the Department of National Defence. However, the process becomes that record requests are then sent to the individual parts of the forces or the Department of National Defence. What that means is that the central nervous system of DAIP, for example, is relying on those record holders to provide that information, and it's almost entirely based on an honour system.

For example, if emails were requested, one of which might incriminate someone or provide context and background that indicates impropriety in a decision, you go to that individual and say, please provide all records responsive to this request. Well, I don't know that they have that email. They may turn over 99 other emails and delete that one email that leads to some degree of culpability or embarrassment, as may be the case. You have to get lucky that someone perhaps is not fully paying attention, or it's not them who might be liable so they disclose everything. There are significant roadblocks in place to ensuring that a fulsome and honest disclosure of these records occurs.

As another example, when members receive requests for information, they are told to provide the search terms that they use: You go to Microsoft Outlook, perhaps, and you type in the search terms related to it. However, those search terms aren't necessarily disclosed unless you file a subsequent request.

I mean, I have an entire list of examples where it's just.... I have incredible amounts of empathy for those who have experienced things far beyond even what I have and may be so traumatized. Little simple things that come back at them, rather than full support and fulsome disclosure, are a barrier that they can't overcome.

● (1655)

Mr. Michael Barrett: I have less than 30 seconds left. I appreciate your answers to my questions.

I'm very curious about your recommendation for a stand-alone study of the ATIP regime within the Department of National Defence and the Canadian Armed Forces. If that's not something you're able to discuss or elaborate on in your replies to other members, I would encourage you to file that with the clerk of the committee in writing at your earliest opportunity so that it might be considered in the evidence we use for our report.

Thank you, Mr. Chair.

The Chair: Thank you, Mr. Barrett.

Ms. Saks, you have six minutes.

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

Mr. White, I would be remiss if I didn't start by acknowledging the courage it takes to come forward to a committee. Thank you for your service.

Sexual abuse is abhorrent. We have an absolute responsibility to victims to make sure that the process they go through in bringing their trauma forward is done with compassion and a sense of transparency, and also a sense of safety. I think it's important to acknowledge that. I speak on my own behalf, but also all of the colleagues in this room, in our absolute support in making sure that safety and transparency are there.

In the context of the study about access to information, you've brought a very sensitive process to light. I'm wondering if you could walk us through the process by which a victim would consider going the ATIP route to be able to access documentation.

There are mechanisms in place within CAF. We have a Minister of Defence who has made it her absolute mission and commitment to make sure that victims are protected through this process. However, since we have you here today, I'd respectfully ask if you could share with us how that currently works.

Mr. Patrick White: Thank you. It is a very on-point question.

My challenge, and what I personally struggle with is.... With regard to the credentials that I explained to the committee earlier, as well as some general familiarity with government processes, I feel relatively comfortable in understanding the ATIP process and the system—how to make a request. However, this is where I go back to highlighting what I was referring to in my remarks.

The system must be designed with the most vulnerable type of person in mind. That could be the 16-year-old who is still in high school. It could be the person who is severely traumatized and wants nothing to do with people in uniform and doesn't understand that there is even a website at all.

The concerns I have are that the understanding.... If you asked the chief of the defence staff or the minister to conduct a poll of members of the forces on their comfort and familiarity with the ATIP system and whether they feel comfortable making these requests, it would not shock me if you had one or two hands in a room full of people and no real genuine understanding of the implications.

I think the problem as well is that there are opportunities for people who make such requests to suffer reprisals. People in the forces, when they note the subject matter of the request or the timing of the request, make guesses as to who has filed that request. It would not surprise me if all of a sudden you would be expecting other administrative actions or changes in things, such that in very subtle and hard-to-detect ways, people are victimized for just trying to use the system.

Ms. Ya'ara Saks: Through you, Mr. Chair, I want to thank Mr. White.

As someone who is a very strong advocate of mental health from a trauma-informed lens, I agree with you wholeheartedly that we need more of that in a whole-of-government approach in many of the things we do.

If you don't mind, I am going to switch to our other witness now, Ms. Francoli.

Thank you for joining us today and for the work that you do on open government and transparency.

In April 2017, you were part of an open letter to the Prime Minister, with many of your colleagues and organizations across the country, indicating that you wished for real change in access to information.

You commented on past witnesses, so you've been following what we've been doing in this study. Do you agree that some of the changes made in Bill C-58 in 2019 are a step in the right direction?

● (1700)

Prof. Mary Francoli: I wouldn't say there is anything fundamentally negative, but I think it was a disappointment to people who are really heavily involved and invested in the access to information regime. So much is happening and there have just been so many studies that say the same thing. Again, it's not that there's a sort of unanimous solution, but there is a lot of commonality.

I think you are seeing it here already with the few witnesses you've had. It's kind of reaching saturation, in a way. There are a lot of the same things being said. Bill C-58 just didn't revolutionize the system in a way that a lot of people were really hoping it would.

It's not bad, just a bit of a letdown.

Ms. Ya'ara Saks: That's fair.

Earlier you mentioned the siloed nature of the ATIP system, its being department by department, and that's certainly something that has come up time and again in our discussions here. What we're seeing is that IRCC is really getting the lion's share of requests at this time.

Would you like to see IRCC officials here, maybe, to comment on what they are facing with the ATIP requests they are getting and how they are managing or struggling with those? You seem to be an action-oriented individual in terms of what you'd like to see, so I'd like your thoughts on that.

The Chair: Could we have a very short response, please?

Prof. Mary Francoli: That would be really interesting. They are typically one of the heavy receivers of ATIP requests. They also have a lot of information holdings and a lot of information holdings that aren't digital, so that makes it more complicated to search.

From the Information Commissioner's testimony, I understand that there may be some interesting things happening there that could impact the ATIP system moving forward. I'd be curious, if I were you, to hear more about that, and I would also like to hear about that, so if you could do it, that would be great.

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

The Chair: Thank you, Ms. Saks.

Thank you, Ms. Francoli.

[*Translation*]

Mr. Villemure, go ahead. You have six minutes.

Mr. René Villemure: Thank you, Mr. Chair.

Ms. Francoli, thank you for being with us today.

I'd like to hear your opinion on the fact that historical records are not systematically released. Is that something that should be considered?

[*English*]

Prof. Mary Francoli: I wouldn't say automatically. There are a number of things that would prevent historical documents from being published. Things related to national security that sit within Library and Archives, for example, all prevent them from being published.

I guess this is where I allude to some of the interesting things that Library and Archives is doing that are outside the scope of access to information. They've had a very interesting system of block review, going through files and boxes of old things that have not been released and just kind of selectively picking out some to see if those batches contain any information that couldn't be released under the act. They have released millions of pages, from what I understand, of historical documents as a result.

[*Translation*]

Mr. René Villemure: Should those records be filed in a way that makes them searchable? Are they currently being stored in a huge pile, making it impossible to find anything?

[*English*]

Prof. Mary Francoli: My apologies, but my audio cut out here.

[*Translation*]

Mr. René Villemure: I'll repeat the question.

Should the records be filed in a way that makes them easy to search? My understanding is that they are currently available, but that it's hard to find what you're looking for.

[*English*]

Prof. Mary Francoli: Should documents be classified in a way that makes them easier to find? I think there are two things we need to think about. The first is how documents are originally classified. There has been a tendency to over-classify things, and then things stay closed.

I think it would be useful to look at a system of declassification, and that's something we are lacking. It's something on which the Information Commissioner has published a special report. I know she's mentioned it in her testimony to this committee before, I think in May, and she mentioned it to us at the NS-TAG as well.

[*Translation*]

Mr. René Villemure: You're talking about declassifying records, but should they be better classified?

● (1705)

[*English*]

Prof. Mary Francoli: I'm sorry, but my earpiece was not working.

[*Translation*]

The Chair: Can you please repeat the question, Mr. Villemure?

Mr. René Villemure: You talked about a system for declassifying records, but should there be a system to classify records? People have a tendency to classify records at a higher level than necessary to cover themselves. Do we need a more formal system for classifying records?

[*English*]

Prof. Mary Francoli: I think there is a lot of guidance for classifying documents. I don't think it's always applied evenly across departments and agencies, and it might not always be well known among the people who need to be engaged in the classifying of the documents in the first place.

I think it really depends on who's classifying and what their level of comfort is in terms of classification. There's a system there for determining what level of classification a document should be. My impression is that it's probably not applied evenly.

[*Translation*]

Mr. René Villemure: The fact that the system, policy or directive exists doesn't necessarily mean that it will have the desired effect. People may not know about it, or they may misinterpret it.

[*English*]

Prof. Mary Francoli: For sure, yes.

[*Translation*]

Mr. René Villemure: Do you think the Access to Information Act should apply to documents covered by cabinet confidence?

[*English*]

Prof. Mary Francoli: That's a hard one, and I think that's kind of divisive among the access community. I think there are a lot of reasons why we want to see that.

I would also say that I understand that decision-making in cabinet is not easy and there needs to be room for discussion and deliberation. People need to feel free to have difficult discussions and to change their minds.

I think that one is a little bit complicated. I can see arguments on both sides. Perhaps that's just an academic wishy-washy answer, but—

[*Translation*]

Mr. René Villemure: They could be disclosed for the reasons we discussed.

Should the Information Commissioner have the ability to look at documents covered by cabinet confidence to say whether they were classified properly? Then, the commissioner would know whether they had been classified appropriately or whether they had been overclassified.

[*English*]

Prof. Mary Francoli: I would say yes. She doesn't have to release them, and she is very careful about that, but I think it's important that there is an oversight mechanism where somebody can look at all of the information involved and then make a decision. I think that's an important point.

[*Translation*]

Mr. René Villemure: Thank you, Ms. Francoli.

Mr. White, what are you hoping to accomplish by appearing before the committee today?

[*English*]

The Chair: Could we have a very quick response, please, Mr. White?

Mr. Patrick White: The first objective, I would say, is a recognition from maybe this committee and anyone interested in the access to information system that there are real barriers to victims, complainants and survivors in accessing essential information, which hasn't yet been a real part of the conversation. I think steps have been taken, but there are still a lot of things that no one has clued into, as in, “Oh, we wouldn't have thought that might be a problem.” I can share that both from personal experience and from what I've heard from others as well.

The second piece is that I think it needs to be looked into further to get a real sense of the scope of the problem or of creative solutions, because action is really what's needed. It's great that we have the laws in place, but if they're not followed or they're flouted, effectively they don't achieve the results needed.

Those are two of the objectives.

The Chair: Thank you, Mr. White.

Thank you, Monsieur Villemure.

Mr. Green, you have six minutes.

Mr. Matthew Green: I have a point of order prior to my intervention, if I could, Mr. Chair.

The Chair: Okay. Go ahead with your point.

Mr. Matthew Green: I want to note that the procedure guide for witnesses states:

> Testimony before a parliamentary committee is protected by parliamentary privilege. This means that witnesses enjoy the same freedom of speech and immunity from prosecution or civil liability as do Members of Parliament.

I want to ask you, Mr. Chair, if we know for a certainty that this would extend to members of the Canadian Armed Forces.

● (1710)

The Chair: Yes, Mr. Green. It expands to witnesses who appear before committees.

Mr. Matthew Green: Thank you.

I'll now proceed with my round.

The Chair: I'll start your time now, sir.

Mr. Matthew Green: Thank you.

I want to begin with Mr. White.

Mr. White, if I heard you correctly, you were of the opinion, in your opening remarks, that your participation here—given the culture of the armed forces—may result in reprisal. Is that correct, sir?

Mr. Patrick White: That is correct.

Mr. Matthew Green: I won't get into specific details about your current participation.

Are you satisfied that what I just read out, in terms of your protections, would extend to you as a witness, or do you still believe the culture of the Department of National Defence would supersede the directions and protections accorded to you by the House of Commons?

Mr. Patrick White: I think the simple answer to that question is that there are a lot of creative ways you can suffer reprisals, which are not easy to link back to testimony at a committee. It could be administrative or a reassignment of duties. These are all things that have been flagged, throughout Operation Honour, as things victims have faced after coming forward.

The best I can say is, it's nice to hear that there are protections, but protections are only as good as that which you can truly enforce.

Mr. Matthew Green: As a member of Parliament, I'm joining the other members here in going beyond just thanking you for your service. It's certainly my intention to ensure that parliamentary privileges are accorded to you by our Standing Orders. The House of Commons would hopefully suffice in providing you with that kind of protection, in terms of whistle-blowing.

What I want to do, seeing how you're coming to this committee with lived experience, perhaps, and anecdotal experience from people you've worked with.... Could you share other jurisdictions or armed forces around the world that may have, in your opinion, more adequate and suitable whistle-blower protections?

Mr. Patrick White: The short answer to that question is that I would have difficulty pointing to those other organizations, as it's outside the scope of what I've studied.

I can say that, from what I understand through other experts—perhaps some of you have heard it at committee or in the news—Canada has an atrocious record when it comes to whistle-blower protection. There is no pot of gold at the end of the rainbow for people who come forward. I understand that even if members in the forces, or the government broadly, are not interested in participating in wrongdoing, they are very willing to look the other way in the interest of putting food on their table or putting their kids through school.

It is incredibly difficult to want to tell anyone. There is no reason or incentive to come forward, unless you have an incredibly strong sense of justice, in terms of what is right. I can assure you there is no benefit or reward that comes from it. In fact, my experience has been that you get a lot of the opposite.

Mr. Matthew Green: I can appreciate that.

I want you to know, for the record, that we are in the midst of 16 days of activism against gender-based violence.

In your opening remarks, you certainly raised the spectre of a whole host of problems. I think you, quite rightly, also identified the ongoing investigations into the culture at the most senior levels of the armed forces and the Department of National Defence. I want to thank you for that, and I hope this committee.... I would say, sir, that you have been successful in flagging this as a very real concern. In a non-partisan way, I would imagine every member of this committee has taken your testimony to be of the utmost importance and seriousness.

I will now reflect on some comments made by Associate Dean Francoli.

You mentioned, in previous testimony, that you were not sure whether the “open by default” policy in place in the U.S. would have any significant effect on open data. I flagged the language used with some folks earlier. It's kind of like a jargon in government. It sounds great, a bit of sloganeering: “open by default”.

I'm wondering whether your opinion is still the same. Is this language around us more words than action, when it comes to governments providing more transparency?

● (1715)

Prof. Mary Francoli: Here in Canada, when we are talking about “open by default” and open data.... We've seen more movement on open data than “open by default”. It's tough, because it involves a bit of what Mr. Villemure was saying. You have to think about the classification of things in advance. It's more like proactively releasing things—making withholding information a rarity and limited to things like national security.

Mr. Matthew Green: Your subject matter expertise is going to be helpful, so why don't we give you the opportunity to create some definitions? If I don't have the time accorded to me, then I would ask that you submit it.

However, in regard to principles of open government, what principles require the greatest improvement given the current access to information regime?

The Chair: You have about 20 seconds.

Prof. Mary Francoli: Okay.

Mr. Matthew Green: If you're willing, maybe you can submit written documents. I just want to make sure that we're defining the terms.

Prof. Mary Francoli: Sure. I'm happy to submit something written, but I'm not sure that I can do it justice in 20 seconds.

Mr. Matthew Green: I may have another round, and if I do, I'll come back to you with that question.

Thank you.

The Chair: You will have another round, Mr. Green.

I want to remind all members that we have some committee business that we need to deal with, so some of the questioning may be a little bit shorter as we get to the later part of the round.

[*Translation*]

You have five minutes, Mr. Gourde.

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

Ms. Francoli, there's a lot of focus on government culture and transparency. From what you've seen of the federal public service, do you think there's one department, in particular, that demonstrates more transparency, a department that could serve as a model?

[*English*]

Prof. Mary Francoli: I think there have been very different types of initiatives. They're hard to compare in many ways, because different departments and agencies are engaging in different functions. I wouldn't necessarily point to one as being the best.

Treasury Board has been leading the open government movement within the government, so that's a good place to look. I would encourage you to call someone from Treasury Board to maybe talk about the transparency initiatives, the Open Government Partnership, and of course how it relates to the access to information system as well.

Access to information was included in some of the early open government work engaged in by the Government of Canada in the context of the Open Government Partnership, and then it kind of fell out of place in the open government action plans.

I know I'm moving away from your question. However, I think it's quite subjective and a bit more nuanced to say that someone is doing a lot better, or one agency or department is doing much better, than the others. They each have their own very different initiatives.

[*Translation*]

Mr. Jacques Gourde: Thank you.

Mr. White, you provided a pretty comprehensive list of recommendations. You talked about the sexual misconduct in the military and the fact that it could tarnish the reputation of the armed forces.

The armed forces are having trouble recruiting new members. Could your recommendations help the military clean up its image and, indirectly, help with its recruitment challenges?

Mr. Patrick White: Thank you for your question.

[*English*]

I certainly believe that in establishing confidence, not just through words but through concrete actions, you can turn a recruitment crisis into a recruiting success. The best spokespeople for the Canadian Armed Forces should be victims who say they have been heard, action has been taken and they strongly encourage every person who is listening to join the forces.

Instead, the response in many cases seems to be reprisal, dismissal and denial of information. To be honest, I wouldn't possibly expect to receive notification [*Technical difficulty—Editor*] that the naval reserve is organizing to have me released from the Canadian Armed Forces.

I don't understand. I've personally tried to share ideas on subjects such as how to promote our military history and recognition of Canada's armed forces among the general public. I can't say that many people in the department, especially the ones with higher authority, have ever really expressed interest in my ideas, at least. I certainly hope that isn't the case for others, but I'm getting the impression it is.

● (1720)

[*Translation*]

Mr. Jacques Gourde: Ms. Francoli, what are your top one, two or three recommendations for the committee?

[*English*]

Prof. Mary Francoli: That's a good question. I have a list here that goes beyond that and reinforces what others have said. Having really good information management—looking at information management systems, including, as one of the previous witnesses said, things like storage, retrieval and digitization strategies for documents to deal with the paper holdings we have and ensure access to old files—helps to build the cornerstone for good access to information. Proper resourcing, a declassification strategy and limiting exemptions are all things I know you have heard about before. As well, we need good leadership and more proactive disclosure. I could keep going.

We need better education on the use of access to information and on how to make requests. That's something I know you have heard before as well. I was thinking of that as Mr. White was talking as well. There's no one to really help you figure out this complicated system if you want to make an access to information request yourself. It's immensely complicated.

[*Translation*]

The Chair: Thank you, Mr. Gourde.

[*English*]

Thank you, Ms. Francoli.

Mr. Bains, online, you have five minutes, sir.

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

Thank you to our guests for joining us today.

Mr. White, thank you for your service and for coming forward and sharing.

I want to start with you. If I can ask, are there any sexual assault cases that you feel have not been pursued because the victim could not get access to the information they needed?

Mr. Patrick White: That's a very difficult question for me to be able to answer outside of my own experience, but I'm fortunate enough to be able to confirm to you that absolutely, yes.

It has been very difficult, and I assure you, without going into further details at this time, that justice has not been served in my own personal circumstances. In fact, I have recently received information that the leadership of the naval reserve may be positioning to make things worse by shutting down further investigations and other things.

Rest assured, if it has happened in my case, as the old expression goes, dollars to donuts it has happened other times, I'm sure.

Mr. Parm Bains: Thank you for bringing that forward.

I will move to Associate Dean Francoli. In your experience, what challenges exist in ensuring the integrity and safety of the data that individuals provide to either a company or, in this case, a government? What safeguards need to be built into the design phase of an application to ensure it will protect users' data?

Prof. Mary Francoli: I'm sorry, but do you mean with the access to information request form itself?

Mr. Parm Bains: Yes.

Prof. Mary Francoli: I'm not sure I'm well placed to answer that one, in terms of protecting the users. For that one, I would suggest you might want to talk to the Privacy Commissioner. I noticed the commissioner hasn't been here yet.

Protecting the privacy of the request, the personal information, is kind of a first-come, first-served system. The analysts are supposed to be addressing them as they come in and not classifying types of requests.

I'm not sure if I'm exactly getting at what you're asking.

Mr. Parm Bains: I will move on. Your research is focused on the way digital media has impacted three broad areas—citizen engagement and mobilization, governance, and access to information and data.

How has digital media impacted access to information?

● (1725)

Prof. Mary Francoli: I think it has had an enormous impact. Part of the issue we face with our Access to Information Act is that it predates digital. It was designed in a mediascape that was very different from the one we operate in today. As a result, instead of starting from scratch and building a piece of legislation that really reflects the contemporary digital media landscape and the types of information holdings we have, we're trying to patch up this old piece of legislation and make it relevant to the digital era, and doing that is tough.

When we look at the Centre for Law and Democracy's ratings of various pieces of access to information legislation around the world, some of the ones we see that come out ahead of ours are ones that are new. They have been developed explicitly to deal with these issues. Just the level of information and data we have available to us now, the way we store that, and the way we fail to keep up information and data holdings as technologies change, as software changes, make it really difficult to have good information management. As I said earlier, that's really the foundation of being able to employ the act successfully.

Mr. Parm Bains: Okay.

This one could be for both of you.

One of our previous witnesses, Monsieur Drapeau, suggested changes for the Information Commissioner to help speed up the process of ATI: specifically, to introduce a one-year period before complaints can be brought before a federal court. What are your thoughts on his analysis?

The Chair: We have five seconds, Mr. Bains.

Mr. Parm Bains: I'll leave it there.

Thank you.

The Chair: I'm sorry. You'll have another chance in the two and a half minutes for the Liberals.

[*Translation*]

We now go to Mr. Villemure for two and a half minutes.

Mr. René Villemure: Thank you, Mr. Chair.

Ms. Francoli, are there countries that are doing a good job when it comes to access to information, countries whose lead we should be following?

[*English*]

Prof. Mary Francoli: I think it's tough, because the country context matters so much when you're talking about access to information.

For example, when we're talking about digital government, Estonia is often referred to. The old CIO used to talk about Estonia a lot. There was a little Estonia craze there for a while. There are tons of interesting things happening there, but for us it just doesn't compare. Canada is so much bigger. Our division of power makes it really complicated.

I think there are things we can learn from other countries, of course, but we have to be careful to not just adopt what works well in another country. We need to make sure that it actually works for us, for our unique national context, and one of the things—

[*Translation*]

Mr. René Villemure: I have to stop you there because I have very little time.

Do you think it's useful for Canada to look to the General Data Protection Regulation or the Australian model?

[*English*]

Prof. Mary Francoli: Yes. It's always interesting to look at other Commonwealth countries. Again, the context here, even though we're part of the Commonwealth, is still a bit different.

One thing that makes things a bit different for us—and this really goes to access to information and open government more broadly—is our Official Languages Act. That's a unique country context that impacts our information holdings and disclosure and that Australia is not dealing with in the same way.

[*Translation*]

Mr. René Villemure: Can you elaborate on the challenge around official languages?

[*English*]

Prof. Mary Francoli: I think the difficulties are.... We want to think about open government initiatives to release information in both official languages at the same time. Oftentimes, the Official Languages Act is actually used as.... It's kind of held up as an impediment to openness in government and to further transparency, as in, “Well, we can't do it because we don't have it translated yet” or “It's too expensive to translate it, so we can't release this information.”

I think the act has been used as a mechanism to circumvent transparency in some cases.

● (1730)

[*Translation*]

Mr. René Villemure: We try to address official languages challenges as best we can for the purposes of our country, but we haven't fixed everything.

Thank you.

The Chair: Thank you, Mr. Villemure.

[*English*]

Mr. Green, you have two and a half minutes.

Mr. Matthew Green: Thank you.

Associate Dean Francoli, I would love the opportunity for you to be able to address the questions in regard to the principles of open government. What principles require the greatest—

The Chair: Excuse me, Mr. Green. Can you turn on your camera, please? We can't see you.

There you go. Thank you.

Mr. Matthew Green: Thank you very much. My apologies for that.

I want to return to Associate Dean Francoli in regard to the principles of open government. What principles require the greatest improvement, given the current access to information regime in Canada?

Prof. Mary Francoli: Open government is really founded on the ideas of accountability, access to information and civic engagement. I would say that those are the three big things that underpin open government.

I think we have a lot of civic citizen participation opportunities. Things are changing, and I think there's been an effort to improve the way that citizens are engaged.

I think access to information is still the big one. In the first couple of action plans to the Open Government Partnership, there were more commitments made around access to information, but I think it's just such a difficult one to move forward. I think this alludes to some of the disappointment I mentioned earlier around Bill C-58. As well, it's hard for public servants to move forward and to get buy-in on change related to access to information. They kind of stopped being included in different commitments on access to information within the action plan.

For me anyway, access to information itself is the big principle of open government that we need to improve here in Canada.

Mr. Matthew Green: What would that look like, specifically, if you had examples for this committee?

Prof. Mary Francoli: I think it would look like a much more significant reform to the Access to Information Act we currently have. If we were being really ambitious, we would establish a transparency strategy that would bring all of these different sorts of open government and transparency initiatives together, so we could see how they work with one another.

There are all kinds of interesting things happening across the Government of Canada. A lot of hard work is being put into open government, all of which is outside the scope of the act. I think, over time, it will hopefully help ease some pressure on the access to information system.

Mr. Matthew Green: Thank you.

The Chair: Thank you, Mr. Green.

We have a round of two and a half minutes scheduled. I'll just remind the committee that we are running over time here.

Mr. Kurek, you have two and a half minutes or less.

Mr. Damien Kurek (Battle River—Crowfoot, CPC): Thank you very much, Mr. Chair. I'll keep this short.

First, thank you again, Mr. White, for your service. I'll just emphasize that access to information is not simply about government accountability. As we heard in your testimony, it relates directly to ensuring that government cannot cover things up. In your case, these are things related to ensuring that victims get justice. Thank you for that.

Dean Francoli, I appreciate your testimony. I'll note here that the namesake of the college you are dean of.... I'm proud he was born in Battle River—Crowfoot. I'm glad to have you before the committee.

I'll simply ask the two quick questions I've asked all our witnesses thus far. A yes-or-no answer will suffice.

I'll start with you, Mr. White.

Is a functioning, strong access to information system needed in a modern democracy? A yes-or-no answer would be great.

Mr. Patrick White: Yes, it's imperative.

Mr. Damien Kurek: Go ahead, Dean Francoli.

Prof. Mary Francoli: I like how you promoted me to dean. That's very kind.

Some hon. members: Oh, oh!

Prof. Mary Francoli: Looking at previous meetings, I anticipated this question. Yes, I would agree, as well.

Mr. Damien Kurek: You might have anticipated the next one: Do you give Canada's current access to information system a passing grade?

Again, I'll start with Mr. White.

Mr. Patrick White: No, and I think the victims and their experiences speak for themselves, on that point.

Mr. Damien Kurek: Okay. Thank you very much.

I'll go now to Associate Dean Francoli—maybe, one day soon, Dean Francoli.

● (1735)

Prof. Mary Francoli: I don't know if I want that job.

If I think of the system in a way that's bigger than just access to information legislation, I would say we pass. If you're asking specifically about the Access to Information Act, I would say, no, we have a ton of work to do.

Mr. Damien Kurek: Okay.

With that, Mr. Chair, I'll hand it back to you. Thank you.

The Chair: Thank you, Mr. Kurek. You're under time, which is appreciated.

The next two and a half minutes are for a final intervention.

Go ahead, Ms. Khalid.

Ms. Iqra Khalid: Thank you, Mr. Chair.

Thank you, Mr. White and Associate Dean Francoli.

I'll be very brief with my question. I have asked other witnesses this.

We heard, in this committee, that the majority of ATI requests are individual file-based—within the immigration department, for example, or others where there are concerns related to individual claimants, etc.

Associate Dean Francoli, I want to know this: How do you think that impacts the overall functioning of the ATI system? Does it take away from the function of ATI when there are thousands upon thousands of claims filed? Does that impede access to information for people who may actually need that access?

Prof. Mary Francoli: I think it creates a huge stress on the system.

It's sad that people can't have access to their information without going through an access to information request, which can be very complicated to navigate. If we think about who's filing a lot of the requests.... IRCC is one of the biggest recipients. CRA is one of the biggest recipients. I'll go back to Mr. White's point: In many cases, we talking about vulnerable people who need to access that information, so I think it's a very sad state that people feel they have to go there.

I'd be curious to hear what IRCC is doing, in particular, to help ensure people can have the information they need without going through this process.

Ms. Iqra Khalid: Thank you.

Is there a recommendation you would propose to this committee, to include as part of the report, as to how to deal with requests for access to information that maybe shouldn't have to go through that process or that could be deemed vexatious or malicious in their intent?

Prof. Mary Francoli: I think those are different things.

To me, if you're trying to access your own information, or access information about a file you have with IRCC, for example, that's not vexatious. You're trying to get something done and move something forward yourself. If you can't do that, I think there should be a complaints mechanism in addition to being able to launch an access to information request.

Vexatious requests are obviously a very specific thing. There is a mechanism—as I'm sure you know—under the current legislation for the Information Commissioner to step in there.

The Chair: Thank you, Ms. Khalid.

Ms. Francoli and Mr. White, thank you for your appearance today in front of the committee. On behalf of all Canadians, I want to say thank you.

Mr. White, I know it has been said several times, but thank you for your service to our nation. On behalf of a grateful nation, we very much appreciate that service.

We have some committee business we need to get to. I'm going to suspend for a minute to give our witnesses an opportunity to leave.

The committee is suspended.

● (1735)

(Pause)

● (1735)

The Chair: I'm going to call the committee back to order.

I understand, Mr. Green, that you have a motion you want to present. I'm going to get to you in a second, if you don't mind. There are a couple of things that I want to bring up.

First of all, we have study budgets that need to be adopted. There are two of them that have been put before you: Roxham Road for $2,425, and the ATIP study for $10,150. I would like to include the ArriveCAN study in that approval process. According to the clerk, it has come in at $8,950.

Can I have consensus on the part of the committee members to adopt those study budgets?

Some hon. members: Agreed.

The Chair: Okay, we'll consider those budgets adopted.

Before I get to you, Matt, for the sake of the committee, as far as the upcoming meetings are concerned, here is what we have scheduled so far.

I will admit to difficulty in procuring some witnesses. I don't know whether it's the time of year. Obviously, there's been the American Thanksgiving. We've had some challenges with some of the requests for witnesses from Amazon, for example.

This Wednesday, we are scheduled to continue with the ArriveCAN study. We have one witness who has been confirmed. We did invite Amazon. They said no. We have invited a witness, to be confirmed as well, from TEKsystems.

On Monday, December 5, we're scheduled to recommence the ATIP study. We have ATIP coordinators from Global Affairs Canada who have been confirmed. To be confirmed, but who have been invited, are ATIP coordinators from the RCMP, Public Safety and the PCO.

On Wednesday, December 7, is the ATIP study. We have three witnesses confirmed who are going to appear in front of the committee on December 7.

I just wanted to bring that to the committee's attention.

I have Mr. Green first.

● (1740)

Mr. Michael Barrett: I have a question.

The Chair: Okay. I'm going to go to Mr. Barrett, if that's okay.

Go ahead.

Mr. Michael Barrett: My question is about what you just raised. In talking about getting witnesses, you said that one of the witnesses we invited said no.

The Chair: I received confirmation tonight that they said no.

Mr. Michael Barrett: Chair, I'd like to take a quick second here, if I can.

We requested that a witness appear. The witness is a contractor for the Government of Canada. They've received millions of dollars of taxpayer money. To not say, well, you know, we have some time challenges.... To say no to a parliamentary committee is absolutely unacceptable.

Ms. Iqra Khalid: I have a point of order, Mr. Chair.

The Chair: Go ahead on your point of order.

Ms. Iqra Khalid: It's common practice for us to discuss individual witnesses while we're in camera. I just want to note that we are in public right now, and I think it's improper to talk about specific witnesses in public.

The Chair: I would agree with Ms. Khalid on that.

Mr. Michael Barrett: Well, I'll move that we take the meeting in camera, then, to discuss this.

Mr. Matthew Green: Point of order.

The Chair: Mr. Barrett, I'm going to go to Mr. Green first. I appreciate your intervention, but Mr. Green did acknowledge to me that he did want to go first. I thought it was on this.

Mr. Green, go ahead, please.

Mr. Matthew Green: Mr. Chair, I say this with the utmost respect for your guidance in this committee. You brought this issue to the committee in open forum. Nothing pursuant to our Standing Orders would require us to go in camera.

What we have is a refusal of an organization to come before this committee. I'm not sure there is anything within the parameters of a discussion that we would have.... These are procedural questions. We talked about parliamentary privilege. We are the grand inquisitor of the nation. We have the power to send for people, documents and evidence.

I would say, sir, that if it is the intention of a motion to move in camera, which I believe is what is required in order to be procedurally in order, the motion be brought to this committee and we vote accordingly, because I would like to go on the record and say that I have no interest in having any conversations about Amazon in camera, given their reluctance...not their reluctance, sir, but their refusal, to come to this committee.

I would ask for that vote to happen.

The Chair: Just to be clear, Mr. Green, and for Mr. Barrett's benefit too, it wasn't an outright refusal. They indicated scheduling issues as being the problem for this Wednesday. I would ask the committee's indulgence to perhaps ask them for another opportunity to come to committee. I think that would be appropriate. The indication I have from the clerk is that they had scheduling issues. So I don't want to go too far into the weeds on this one.

Go ahead, Mr. Barrett.

● (1745)

Mr. Michael Barrett: I'll be very brief, Mr. Chair.

I am willing to take a step back on this, but then I would ask that in going back to them with another date, the clerk be asked to remind the witness that the committee does have the powers to send for people, papers, and evidence, and that we do hope they respond to our invitation so that it can be on those terms.

The Chair: That's a fair point, Mr. Barrett.

I'll go to Mr. Green now.

Mr. Matthew Green: Thank you very much, Mr. Chair.

I do have a motion that has been sent to the clerk and I believe also to the P9s of members of the committee. It's a housekeeping issue. I think we've all received correspondence on some of the frustrations people are having around the scheduling.

Before I move this motion, for those who are watching, I want to say that this is not in any way, shape or form reflective of our clerk's attempts and abilities to schedule people. This is not in any way, shape or form an attempt to minimize the study or to undervalue the expert testimony. This is just a situation we have that's seasonal.

Mr. Chair, the motion is as follows:

> That, in order to allow for witnesses to be scheduled with sufficient notice and time for preparation, the committee pause its study on the Access to Information until January 30, 2023; and, that the committee invite the Commissioner of Lobbying of Canada, the Privacy Commissioner of Canada, and the Information Commissioner of Canada to appear as part of a committee study on supplementary estimates (B) 2022-23; and that the commissioners appear at committee no later than December 6, 2022.

For obvious reasons, Mr. Chair, we need to have the supplementary estimates dealt with here. This would be a good opportunity to invite these folks while we allow our clerk to go out across the country and adequately schedule subject matter expertise for our ATIP study in a way that I think is reflective of the seriousness and importance of the study.

The Chair: Thank you, Mr. Green. The motion is in order.

There are a couple of issues I do want to bring up to you and to other members of the committee.

As I mentioned earlier, we do have a couple of ATIP study meetings that have scheduled witnesses to appear. These are witnesses who were asked to appear. The only time they could be scheduled was December 7, for example. We do have those meetings already in place.

The clarification I would need from you, Mr. Green, is whether you want all three of the commissioners to come in a singular meeting on supplementary estimates (B).

The other thing I would propose to you is that the deadline.... We don't know; it could be as early as later this week. The committee can always consider the subject of the supplementary estimates at a later date. We can do that.

I just need clarification from you, Mr. Green, on whether you want all three here at the same time or separately. We can accommodate to have all three of them here at the same time, but separately it would take up three different meetings.

Mr. Matthew Green: To your first point, I would say that I feel the ATIP study is best scheduled in a lexical order that helps us provide the most important primary testimony first. I find that it's helpful in studies, particularly of this nature, to be informed by subject matter expertise, government staff, ministers and that type of thing up front, and to then get into other, more ancillary witnesses.

I'm not sure that was the case—and I say that respectfully—in terms of today's intervention, so I would say that we do put it on pause until the new year and then allow the clerk and you, sir, to work out a work plan that has, to the best of our ability, a lexical order of operation.

As it relates to the commissioners, I'm certainly fine to have them all in one meeting, but I would leave that up to the discussion of the other committee members around the table.

● (1750)

The Chair: The motion is on the floor for debate, but I'll go back to you.

This is where I need clarity, because we do have witnesses who are already scheduled to appear. Those schedules have been accommodated for December 5 and December 7. If with this proposal we put off these meetings, then we're also going to be putting off those witnesses, who, by my understanding, are anxious to appear and who have made their schedules available for those two dates. That's the challenge I have.

Mr. Matthew Green: Are they ministers who are coming?

The Chair: No.

Mr. Matthew Green: Are they senior government staffers who are coming?

The Chair: I don't have their backgrounds in front of me, Mr. Green. Just give me a second.

Mr. Matthew Green: Sure.

The Chair: I just got some clarification from the clerk.

We have senior government officials who are coming on December 5, first from Global Affairs Canada. On Wednesday, December 7, we have reporters who are coming to speak about the ATIP issue. There were attempts made to accommodate their schedules earlier. These were the earliest and most viable dates when they could come.

That's how the schedule was made out, Mr. Green.

Mr. Matthew Green: Then I would say, Mr. Chair, without trying to be difficult, by all means, if it's the will of the committee that we pursue those two days, that's fine.

I just received, like we all did, some frustration from the public that they felt this was being rushed and that folks weren't getting adequate notice. I wanted to go on the record today to assure people that this is not the case and that we will work through this study thoughtfully and give people the ability to prepare.

If you've already done that for those two days, then I would totally concede that point and be amenable to bumping the date within the context of this to allow for that to happen.

The Chair: Okay.

Mr. Green, again, just for clarity, I am certainly not averse to inviting the commissioners. If we wanted to do so, we could probably do it on December 12 at our scheduled meeting, if you would like to do that. I can accept the motion, but “no later than December 6”.... I think if we put a date on it as December 12, why don't we look at that, then?

I see a thumbs-up from Mr. Green. I also see that Mr. Kurek's hand is up.

Mr. Damien Kurek: Yes, I just want to acknowledge that if we go too much longer here, I think there will be a resource issue, so I'd be happy to move an amendment that whatever the clerk feels and whatever is amenable to Mr. Green.... I agree with the spirit of his motion, however we ensure that we get that sorted and then make sure we're not taking away resources from other committees as well.

The Chair: I'm sorry, Mr. Kurek. I was just talking to the clerk. Could you repeat what you said? I'm sorry about that.

Mr. Damien Kurek: Let's just get it sorted. I'm supportive of the motion. If an amendment is needed, count me in, as long as it's in the spirit of what Mr. Green's motion is. I'm concerned that if we drag this out too long, other committees will be affected.

The Chair: If it's okay with you, Mr. Green, we're looking at December 12 to have the commissioners come in to look at the supplementary estimates.

Is that correct?

● (1755)

Hon. Greg Fergus: That's correct.

The Chair: Members are good with that.

I see your hand, Mr. Fergus.

The last thing I want to bring to the attention of the committee is that we received a letter from the commissioner on the new edition of the “Lobbyists' Code of Conduct”. It's not an order of reference from the House, but members are welcome to study that in the future if we need to. I know that the commissioner has made herself available, as I said, in December at some point. It's something to consider—maybe not right now, but later—and we may want to have the commissioner here to discuss that as well.

Mr. Fergus, go ahead.

Hon. Greg Fergus: Are you going to be adjourning the meeting?

The Chair: I will be adjourning the meeting.

I thank everybody for their patience. This is my fault and I'll tell you why. It is because I was really benevolent with the time on that first panel. I was listening more than I was watching my clock. That won't happen again.

The meeting is adjourned.