HOUSE OF COMMONS
CHAMBRE DES COMMUNES
CANADA

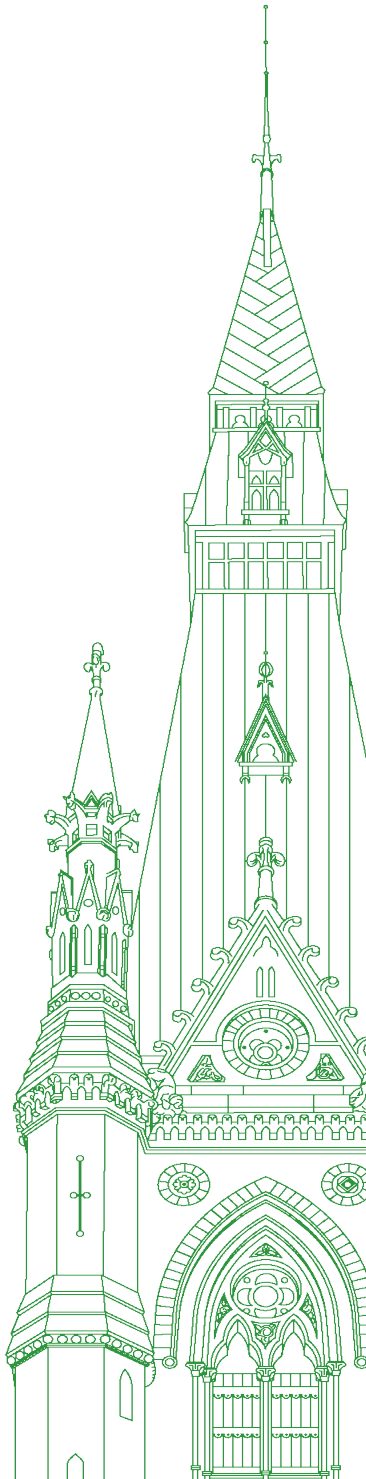
44th PARLIAMENT, 1st SESSION

Standing Committee on Access to Information, Privacy and Ethics

EVIDENCE

NUMBER 033

Tuesday, August 9, 2022



Chair: Mr. Pat Kelly

Standing Committee on Access to Information, Privacy and Ethics

Tuesday, August 9, 2022

● (1505)

[*English*]

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

I'd like to welcome everyone to the 33rd meeting of the Standing Committee on Access to Information, Privacy and Ethics. Pursuant to Standing Order 108(3)(h) and the motion adopted by the committee on Tuesday, July 26, 2022, the committee is meeting to study device investigation tools used by the Royal Canadian Mounted Police.

Today's meeting is taking place in a hybrid format, pursuant to the House order of Thursday, June 23, 2022.

Today we have three witnesses on this panel. We're pleased to have Ronald Deibert, professor of political science and director of the Citizen Lab, Munk School of Global Affairs and Public Policy, University of Toronto. We have Brenda McPhail, director of the privacy, technology and surveillance program at the Canadian Civil Liberties Association. We are also expecting Michel Juneau-Katsuya, researcher on national security and intelligence. My understanding is that we are in the midst of navigating some technical issues with this witness, so we will proceed with opening statements from the other two. We certainly hope to have our third witness here in time for him to deliver his opening statement.

With that, I will ask for Professor Deibert to begin.

You have the floor for up to five minutes.

Mr. Ronald J. Deibert (Professor of Political Science, and Director, Citizen Lab, Munk School of Global Affairs and Public Policy, University of Toronto, As an Individual): Thank you, Mr. Chairman.

I am Ron Deibert, professor of political science and the founder and director of the Citizen Lab at the University of Toronto's Munk School of Global Affairs and Public Policy.

Since 2001, the Citizen Lab has researched information security issues, and one of the principal areas of our research has been the mercenary spyware industry, in which private actors sell hacking services to governments. We are widely recognized as one of the world's leading authorities on this topic.

My staff and I have testified or provided briefings numerous times to the U.S. White House, the Department of State, Congress, the European Parliament and other governments on this topic. I'm very pleased to be speaking about it for the first time before a Canadian House of Commons committee.

Today, I want to highlight several themes that arise from this research.

First, the mercenary spyware industry is very poorly regulated and is proliferating quickly. The industry lacks public accountability and transparency. It thrives in the shadows of the clandestine world and is spreading fast without proper controls.

Second, we have documented extensive harms and abuses in just about every jurisdiction in which spyware is deployed. Governments routinely use spyware to hack civil society, political opposition, journalists, lawyers, activists, family members and other innocent victims—both domestically and abroad—including victims living here in Canada.

Third, the mercenary spyware industry is not only a threat to civil society and human rights; it is also a threat to national security. We've observed heads of state and senior government officials who have had their phones hacked with spyware. Not long ago, we notified U.K. authorities about a device we observed being hacked at 10 Downing Street, the residence of the Prime Minister. In short, our 10-plus years of research show that the spyware industry is one of the most serious threats to civil society, human rights and democracy today.

The recent revelation about the RCMP using spyware raises serious concerns.

First, spyware is not like a traditional wiretap; it is more like a wiretap on steroids. Advanced spyware is to surveillance as nuclear technology is to weapons; it represents a quantum leap forward in sophistication and power. The latest versions provide silent and unfettered access to a target's entire pattern of life. Despite these nuclear-level capabilities, it is remarkable that there has been zero public debate in Canada prior to the RCMP's recent revelation.

Second, the threshold for use, oversight, transparency and public accountability must be much higher than for a traditional wiretap. This is especially critical because the RCMP and other security agencies in Canada have a well-documented history of abuses and discriminatory practices.

Third, we need transparency with respect to where Canadian agencies are procuring this technology. Yesterday, the Minister of Public Safety would not acknowledge to this committee from which vendor or vendors the Canadian government purchased spyware. There is absolutely no reason why that should not be disclosed, and there are plenty of good reasons that it should. Our procurement should be transparent and include rules for vendors so that we do not purchase from—and help enrich—firms that sell to governments abroad that threaten Canada's values and security.

Fourth, there are serious public safety concerns around the very existence of this technology. Mercenary spyware is founded on the discovery of software flaws that the software vendors themselves are unaware of or have not patched. The very use of this technology fuels a market that exploits collective insecurity on all of our devices. Canada's overall process, such as it is, to weigh the equities around these trade-offs is poor and opaque.

Fifth, the RCMP's quiet revelation sets a very bad example for the rest of the world. The Canadian government purports to protect human rights and stand for rule of law and democracy around the world. In adopting this technology without public debate and proper limits, we're essentially signalling to the world that we do not really care about these principles.

I will close my remarks with seven specific recommendations.

First, hold public hearings on the threats of the mercenary spyware industry, especially since Canadians have been victims.

Second, if Canadian agencies are going to use spyware, public consultation should be held, and the government should develop a legal framework that is compliant with the charter and international human rights law.

Third, Canada should develop strong export controls for the Canadian surveillance industry. Currently, there are none.

Fourth, Canada should penalize spyware firms that are known to facilitate human rights abuses abroad modelled after those in the United States.

Fifth, Canada should issue clear and forceful statements at the highest levels, for example, from the Prime Minister, Minister of Public Safety and Minister of Foreign Affairs, that we take this threat seriously.

Sixth—

● (1510)

The Chair: You're significantly over time. Go quickly, please, on the last two.

Mr. Ronald J. Deibert: Sixth, Canada should impose a lifetime ban on those who have worked in our security agencies from ever working with mercenary spyware firms.

Last, Canada should make public which firms they are contracting with and develop procurement guidelines for Canadian agencies so they never contract with firms that are connected to human rights abuses abroad.

Thank you, Mr. Chairman. My apologies for going over.

The Chair: That's all right.

Next I will ask Ms. McPhail to begin with her opening statements.

Ms. Brenda McPhail (Director, Privacy, Technology and Surveillance Program, Canadian Civil Liberties Association): Thank you for inviting the Canadian Civil Liberties Association to appear before you today. I'm grateful to the committee for commencing this study of the RCMP's use of on-device investigative technology, because it's an issue of national concern that is also a symptom of a larger problem of inadequate oversight and accountability when police acquire and use advanced surveillance technology.

The revelations about ODIT are just the latest in a series of similar media-led reveals regarding invasive techniques, from social media monitoring to cell site simulators to the illegal Clearview AI facial recognition. This isn't a one-off problem; it's a pattern pointing to a crisis of accountability.

Operational secrecy is a legitimate need in specific investigations. Secrecy around policies that apply to categories of dangerous surveillance technologies is not legitimate in a democracy. We must not allow law enforcement bodies to conflate one with the other to avoid accountability.

Why are these technologies dangerous from a civil society perspective? This committee is aware of the basic risks to privacy rights, so I'll focus on three other reasons.

First, our government agencies are encouraging an industry known for prioritizing profits over human rights and feeding the worst impulses of authoritarian governments. I work with a network of global civil liberties organizations where many of my colleagues see Canada as a role model on issues of law enforcement and due process. This kind of revelation diminishes our international reputation, not just at the level of governments but also on the ground.

Second, using these tools encourages law enforcement, as Professor Deibert noted, to exploit vulnerabilities in the technologies we all depend on, rather than to help get them fixed. We've known for some time that the CSE has duelling accountabilities in relation to their active cyber mandate and their responsibility to protect our cyber infrastructure. Now we know that the RCMP has a similar conflict. This is making us all a bit less safe daily in the name of public safety.

Finally, there's a question of due process. Your witnesses yesterday noted that an agreement detailing the ways the technology has to be protected is a condition of its use. What impact does that agreement have on court disclosures? Are cases ever not taken forward because to do so would reveal details of the technology? In other words, how does operational secrecy compromise the pursuit of justice?

Those are some of the problems. What are the potential solutions?

First of all, I do believe we need a moratorium. This study is just the beginning of an important public conversation we need to have in Canada. If it's true that this technology is a last-resort option, there can't be that much of a risk to public safety to pause its use briefly—certainly not when weighed against the privacy and due process rights at stake as well as the social and diplomatic impacts of the Canadian government condoning the sale and use of spyware.

Then we need to get back to basics, and the basic question isn't "How do we make sure the RCMP or any other body uses these tools lawfully?" Rather, it must be, "Is the use of such tools necessary, proportionate and in keeping with Canadian values?"

It probably won't surprise you that I think it is not. I think we should include, like Europe and the United States have done, the potential for a ban on state purchase of this kind of spyware technology in those conversations we need to have, but if it is democratically debated and determined that it is fit for a narrow purpose, the second question we then need to turn to is how to make the concept of lawful use more meaningful by updating our laws to appropriately govern the decisions to purchase and use these technologies, and to provide transparency and accountability sufficient to engender public trust.

For those laws to be good enough, we need stringent and effectively enforced import and export controls and limits. We need a system where decisions about using controversial potentially rights-infringing technologies can no longer happen behind the scenes. For that, we need not just mandatory privacy impact assessments but should also consider the creation of a truly independent advisory body working with appropriate transparency specifically to evaluate and set national standards for the procurement and use of surveillance technologies, as they have done in New York State.

We would also need public reporting obligations on the use of ODITs. The "Annual Report on the Use of Electronic Surveillance", which has been repeatedly mentioned as an accountability measure, is insufficient. The tools used for this surveillance matter. That's why we're having this conversation. Yet that report simply gives statistics for any audio or visual surveillance. This leads to a final point.

Only one warrant application of the 331 in that report was refused between 2016 and 2020. That suggests that we need a public interest amicus present at those applications to provide a counterpoint to police positions. There are more problems and more solutions, but my five minutes is up, so I look forward to your questions.

● (1515)

The Chair: Thank you.

Although I can't see him on the screen, let me ask, do we have witness Michel Juneau-Katsuya?

No? Are we in touch with him, though?

We're in contact with him. Okay.

Well, we may not get an opening statement from witness Juneau-Katsuya.

We will have to begin our questions.

Mr. Bezan, I would ask you to lead us off.

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

I want to thank our witnesses for joining us today and for their expertise on this.

To both Professor Deibert and Ms. McPhail, have your organizations studied in depth which vendors are potentially being used here in Canada—those who sell spyware?

Mr. Ronald J. Deibert: Which one should go first?

Mr. James Bezan: It's your choice.

You have your mike on, Professor. Why don't you lead off?

Mr. Ronald J. Deibert: Sure.

We have extensively documented spyware vendors around the world. Unfortunately, we lack transparency on the answer to this question here in Canada. There is no public information available to any of us as to which vendors the government is procuring from. As I mentioned in my comments, this is very problematic.

As you heard yesterday, when asked pointedly about this question, the Minister of Public Safety declined to answer. I don't think that's a legitimate answer.

Mr. James Bezan: Ms. McPhail...?

Ms. Brenda McPhail: We have not done that research.

Mr. James Bezan: Okay.

Ms. McPhail, you mentioned in your opening comments the concern that maybe the RCMP hasn't proceeded in the prosecution of certain criminal cases or national security threats because they would have to disclose that they used ODIT. Do you have any proof of that, that they would rather not prosecute to protect the technology?

Ms. Brenda McPhail: There was a case in the past called Project Clemenza, where it was revealed that a number of prosecutions were dropped rather than reveal the fact that a key to access encrypted communications had been obtained by law enforcement. That's the only example I know of, but the mention of a specific agreement, which your witnesses yesterday described as constraining the use of the tools and what could be said about them in public, does give rise to concern about appropriate disclosures in court.

Mr. James Bezan: Do you believe the failure of the RCMP to go forward with that prosecution was because they didn't have a proper warrant that they used to collect that information on those individuals, or that they did so under other mechanisms, such as national security?

Ms. Brenda McPhail: Anecdotally, I'm led to understand that it was done to protect the use of the tool, not because correct warrants weren't acquired.

Mr. James Bezan: Okay.

You know, often when I've travelled abroad, I've been briefed by the Department of Foreign Affairs officials or Department of National Defence officials about the potential of having my cellphone hacked, and that the camera and microphone could be turned on at any time. Do you believe we need to take extra precautions here in Canada as parliamentarians, as people who work on the Hill, in that our government-issued phones could potentially be hacked by not just foreign actors but others domestically as well?

I'll give that to both Ms. McPhail and Professor Deibert.

Ms. Brenda McPhail: I do think it's a concern, but I also think Professor Deibert is best prepared to answer this question.

Mr. James Bezan: Go ahead, Professor.

Mr. Ronald J. Deibert: Yes, I think it's a major concern. The fact of the matter is that you have devices that are highly invasive and tend to be poorly secured overall, given the nature of the digital ecosystem that we live in, next to an industry that, as I've described, spends millions of dollars to identify software flaws without disclosing them to the vendors in order to provide this hacking as a service. We've also documented numerous cases of government officials and even heads of state having their devices hacked with the most advanced spyware. As I mentioned in my opening remarks, we observed a hack device at 10 Downing Street, the residence of the Prime Minister, and reported that to the U.K. authorities.

Really, no one is immune from the most advanced types of spyware. There are no international regulations. It's proliferating widely to governments around the world.

● (1520)

Mr. James Bezan: Professor, from the research you've done, do you believe that, although it would be unethical, employers, including the Government of Canada, would be able to get the clearance to use spyware as a way to monitor employees and people of interest who have government-issued or company-issued devices? Would there be a loophole where they could get around having to apply for warrants because it would be property owned by the employer?

Mr. Ronald J. Deibert: Well, that's an interesting question. I know that there are all sorts of rules. Usually disclosures are made when anyone uses a device within an institution, public or otherwise. If it weren't disclosed, I would certainly say that it would be highly unethical and possibly illegal.

I think Ms. McPhail would be better positioned to answer that question on legal grounds.

The Chair: You do have a few seconds, Ms. McPhail, if you'd care to answer.

Ms. Brenda McPhail: I think a number of different interacting legal instruments would be relevant in that situation. They'd have to be examined carefully to really determine what kind of loopholes there might be.

The Chair: Thank you.

We will now go to Ms. Hepfner for up to six minutes.

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

Thank you to our witnesses for being here today and for providing their testimony.

Mr. Deibert, I want to go back a little bit to your opening statement. You've been talking about how governments use spyware to hack people's phones. You mentioned that this has happened here in Canada. I'm wondering if you could get into a little bit more detail about the cases that you know of. What governments are involved in hacking? What cases have we seen here in Canada?

Mr. Ronald J. Deibert: Certainly. Thank you for that question.

In 2018 we observed that Saudi Arabia was undertaking espionage. We could observe, based on our network monitoring, that there was a hacked device in Quebec. We ultimately discovered that the person whose device was hacked was a Canadian permanent resident named Omar Abdulaziz, who was a very close friend and confidant of Jamal Khashoggi. We published our report on October 1, 2018. The very next day, unfortunately, Jamal Khashoggi was apprehended and brutally executed at the Saudi consulate in Turkey.

We have also documented extensively other Canadian refugees and immigrants who have had their phones either targeted or hacked by foreign governments abroad as part of a growing number of cases that we call “digital transnational repression”.

The long and short of it here is that Canadians are definitely not immune to this worldwide risk that is growing in leaps and bounds, which is precisely why I think we need to be entering into this very serious conversation with a much more comprehensive approach than we have been to date.

Ms. Lisa Hepfner: Okay. Well, I agree that it's a good conversation to have, so what do you mean by a more comprehensive approach? How can we protect ourselves against these international bad actors?

Mr. Ronald J. Deibert: First of all, as I said in my recommendations, I think we need to understand that we have an obligation to do more than just speak words about this topic. In fact, I wish we even spoke words about it. Really, I've seen nothing coming out of the ministry of foreign affairs or from the Prime Minister equal to the level of statements coming out, just to give one example, of the United States and the Biden administration. At the highest levels, the White House and the state and justice departments have all made very powerful statements. They have held inquiries and have started to penalize firms, recognizing the very serious gravity worldwide of this problem that's both a human rights issue and a national security issue.

I could reiterate my recommendations, but I think we need to begin with the fact that we have no export controls for Canadian firms that sell surveillance technologies abroad. That needs to change. We need to be more transparent about from whom we are procuring this technology. As you heard yesterday, the Minister of Public Safety wouldn't even acknowledge who they're buying this from. There's no operational security reason why we shouldn't do that, and there are many good reasons why we should. That's because our procurement is a lever on the industry. If we're going to spend millions of dollars buying this technology, which is very expensive, by the way, we can impose conditions on the firms to say that we're not going to buy from firms that have been widely associated with gross human rights violations both abroad and here in Canada unless they comply with certain standards.

● (1525)

Ms. Lisa Hepfner: What we heard from the RCMP is that they would be releasing secrets to the criminal world if they were to release the technology that the RCMP uses. I don't know what the reasoning is behind that.

What we do know, or what the RCMP says, is that they've used this for specific, targeted reasons, for things like terrorism, murder, kidnapping and trafficking investigations. It was done with a lot of judicial oversight, with many warrants required and where specialized police departments get involved. This has been since 2017.

What's your reaction to that, based on what we know from his study and what we've heard on the record about the RCMP's use of this technology to date?

Mr. Ronald J. Deibert: I would say that security is a very serious thing, and we all need to protect ourselves from the threats that you're describing. Our law enforcement, intelligence agencies and armed forces need to be properly modernized and equipped, and there needs to be judicial oversight. It's reassuring that we heard that it was used for these types of cases and that there was a warrant for it.

Just because we're being told there's a warrant, it isn't a magic wand that makes everything else go away and that we should say, “Don't look any further here.” As I said, there's really no reason why you cannot disclose the vendors from which you're purchasing this technology.

We do not want to have taxpayer money going to some of these rogue, mercenary companies that are contributing to human rights violations abroad and national security problems here in Canada.

Ms. Lisa Hepfner: I guess what it comes down to is that there's no proof that the Canadian government has been using this spyware. All we have on the record here is that the RCMP has used it in certain circumstances, under judicial oversight, to go after specific, serious crimes.

Mr. Ronald J. Deibert: From what I heard yesterday and in reading the news, I'm hearing something different.

First of all, this revelation seemed to come kind of sideways. It wasn't really done in a forthright manner. I also heard that the Office of the Privacy Commissioner was not briefed on this. I also heard, over the last couple of days the numbers changing.

As you heard from my colleague, Ms. McPhail, there's a pattern of law enforcement in this country using investigative techniques and surveillance technologies and disclosing them after the fact. That's not the way you build public trust in law enforcement in a country. We are better than that.

The Chair: Thank you.

With that, we will now go to Mr. Villemure.

[*Translation*]

Mr. Villemure, over to you for six minutes.

Mr. René Villemure (Trois-Rivières, BQ): Thank you, Mr. Chair.

I'm going to start with Mr. Deibert and then move on to Ms. McPhail.

The reason we have undertaken this study is so that the public does not lose its trust in the RCMP. We were somewhat forced to believe what the RCMP told us yesterday—as is the public—because we don't have the ability to take a deeper dive into the issue.

For information purposes, I'd like to ask you a question, Mr. Deibert.

Is it possible to trust when you're forced to trust?

[*English*]

Mr. Ronald J. Deibert: My answer to that would be to invoke someone that you'll remember—and we're showing our age here—Ronald Reagan, who, in response to Mikhail Gorbachev said, "We need to trust but verity." I think this applies to all of our security agencies. In a liberal democracy, it's essential that you have robust safeguards, oversight mechanisms, public accountability and transparency.

What we are seeing here is clearly failing that. If you compare it with what's going on in other countries it's not setting a very good example. It's in line with some of the flawed democracies around the world.

I think we need to have a much more robust net cast over all of this if we're going to use this type of technology, which, by the way, is like a quantum leap in capabilities. What we're talking about here is much different from a wiretap because a device provides a window into every aspect of a person's life and those around them.

As I said in my remarks, this is nuclear level surveillance technology. We need appropriate safeguards to match that sophistication and power.

● (1530)

[*Translation*]

Mr. René Villemure: You wouldn't agree then, that—

[*English*]

The Chair: Monsieur Villemure, I'm pausing your time. I'm going to offer you the option to continue with your round now or we'll pause. You'll have four minutes and 10 seconds left and we can go straight to getting the opening remarks from Mr. Juneau-Katsuya.

Mr. René Villemure: We'll get the remarks, I guess.

The Chair: It's up to you.

Mr. René Villemure: Please go ahead with the remarks.

The Chair: Then at this point I would like to welcome our third witness. I hope we have all of our technical problems sorted out.

Welcome to committee. I will permit you now to make your opening statement for up to five minutes.

Mr. Michel Juneau-Katsuya (Expert and Researcher on National Security and Intelligence, As an Individual): Thank you very much.

[*Translation*]

Please accept my apologies for the technical delay.

Thank you, Mr. Chair and members of the committee, for inviting me and for giving me the opportunity to speak with you about an important issue, one that opens the door to many others.

Allow me to begin by summarizing my thinking, which is based on my over 40 years of experience serving this country and working in the private sector. This also ties in with my research and my work in the national security field.

When it comes to the use of one or more technologies that make it possible to intercept conversations or obtain information protected under the Privacy Act, I would say your examination revolves around four key things: relevance, lawfulness, legitimacy and accountability.

Right off the bat, I want to underscore the importance of protecting privacy as defined in Canadian laws and the charter. Privacy protection is one of the cornerstones of a healthy democracy, and without it, there can be no democracy.

That said, my remarks will focus on three points, which I will come back to.

First, the idea that the end justifies the means is not an acceptable argument when conducting criminal or national security investigations.

Second, partisan games have no place in this debate. It is the fruits of your collective efforts that will help to better protect democracy and Canadians.

Third, this committee has been tasked with a tremendous moral and ethical responsibility. By that, I mean building the necessary tools into the legal framework—the tools the men and women entrusted with our protection need to protect us adequately while respecting the underpinnings of our legal system.

[*English*]

My first point is that one major trap for anybody responsible for collective safety is to believe that the end justifies the means. It is the most dangerous deception that law enforcement officers are facing in the maze of bureaucracy and court systems. Eager to accomplish their work of protecting us and wanting to stop criminals and terrorists ready to harm us, some officers might be tempted to go around the law.

Our own Canadian history teaches us the mistakes of the sixties and seventies, when the RCMP was put in charge of stopping communist agents or separatist zealots. In the name of protecting us, RCMP officers broke the law, believing they were doing the right thing. They were misled and wrong.

I have listened and paid attention to the testimony given to you in the last days. I did not see or hear history repeating itself. I saw officers, under the pressure of not jeopardizing operational or tactical capabilities, who were answering your questions, I believe, to the best of their ability and as much as possible. Thanks to your important work, it is evident that we can enhance the approval process by improving consultation with the Privacy Commissioner, the reporting and evaluation mechanisms and the law itself.

In addition, I was pleased to hear that the court system has kept in place the checks and balances. That is good news and gives us hope that we are on a good track to improve our democratic system and accountability process.

● (1535)

[*Translation*]

The second point I mentioned concerns me more, given the troubling way I have seen certain members of the committee behaving. To ask questions, even tough ones, is a committee member's job and responsibility. Committee members should, however, abide by an overriding principle: their duty is to protect and promote the country's interests, not partisan interests or political agendas. The place to ask questions about technical, tactical or strategic capabilities is in camera.

[*English*]

We shall not forget that the hearings of this committee are public. Some of the bad guys, being criminals or foreign agents, are listening and taking notes. Asking questions while pushing to get, for example, the country of origin of a technology that must remain secret is to serve on a silver platter to the bad guys the means to counter tactical capabilities. To continue making fake allegations of mass surveillance when there is no evidence of it is misleading and dividing our society. Thirty-nine cases and 41 devices spread over more than five years is not mass surveillance.

[*Translation*]

As I mentioned at the outset, I have been watching and analyzing threats against society and Canadians for over 42 years. I was among those who served in the RCMP and dedicated themselves to protecting this country and its citizens. I have experienced the frustration and success that come with conducting an investigation and trying to stop criminals, spies and terrorists from doing us harm, both individually and collectively. I cannot adequately put into words just how an investigator feels when a bad guy gets off because of a flaw in our democratic or legal system.

Yesterday, Philippe Dufresne spoke to you about—

[*English*]

The Chair: I'll have to ask you to wrap up. You're quite a bit over time.

Mr. Michel Juneau-Katsuya: I have three paragraphs left.

[*Translation*]

Thank you.

[*English*]

The Chair: Maybe condense them.

Mr. Michel Juneau-Katsuya: Okay, I will resume.

Mr. Dufresne himself yesterday stressed the importance of stressing the public interest or working on the public interest. Trust today is more crucial than ever for both our democratic system, which you represent, and the law enforcement and security agencies that work hard for us.

[*Translation*]

Thank you for listening. I hope you won't hold my comments or warnings against me; they were necessary.

[*English*]

Your work is important to correct these trends and to muster the greater attention the population is asking for.

The Chair: Thank you. I'm really going to have to let Monsieur Villemure resume his questions.

You have four minutes and 10 seconds. Go ahead, Monsieur Villemure.

Mr. Michel Juneau-Katsuya: That's too bad; it was good text.

Some hon. members: Oh, oh!

The Chair: I believe it, but the time is—

[*Translation*]

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

I was actually talking to Mr. Deibert about trust.

This brings me back to my main point. Do the RCMP's actions serve to maintain trust or, on the contrary, arouse doubt?

Mr. Michel Juneau-Katsuya: Is that question for me, Mr. Villemure?

Mr. René Villemure: Yes, let's start with you.

Mr. Michel Juneau-Katsuya: I think the RCMP's actions are in fact really important in order to gain and keep the public's trust. The accountability and consultation mechanisms as well as the legal safeguards in place are needed to keep and strengthen that trust.

I would say lessons have been learned from the various situations that happened previously. The answers the committee heard yesterday, in particular, the thoughts Mr. Dufresne and others shared, will go a long way toward helping the committee make the right recommendations.

Mr. René Villemure: Thank you.

Mr. Deibert, for the benefit of the general public, who may not fully understand all the ins and outs, can you explain what spyware is capable of?

[*English*]

Mr. Ronald J. Deibert: We have been studying many different types of spyware, and the most advanced ones allow persistent access to a target's device, which, in turn, allows them to do anything on that device, and more than a user can do without the user knowing. Some of the latest versions of this spyware employ what's known as zero-click versions, meaning that there's no need to trick a target into clicking on a link of a fake message. A user, a government client of spyware, can simply issue a command to take over any device in the world that's vulnerable to this type of exploit.

Once inside a device, you can intercept and listen to any phone call. You can read emails and text messages—even those that are encrypted. You could silently turn on the camera and microphone; you can review all of the contacts; you can alter files on the device; you can access a person's cloud account; and you can track their location. It is extraordinarily powerful surveillance technology.

Keep in mind that we live in a different time than even 20 years ago, when a wiretap was something you put on a landline, or you'd place a bug or a GPS tracker in a suspect's car. This gives you all of that and more, because these devices are designed by their manufacturers to be as invasive as possible. They're designed, as well as the apps contained in them, to track every aspect of our lives, so this is a gold mine of information that is available to clients of spyware.

● (1540)

[*Translation*]

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

Yesterday, we heard about warrants and the fact that a judge had to approve and authorize the use of these investigative tools, under part VI of the Criminal Code. It's a good oversight mechanism, it would seem.

I'm not sure whether you agree with me that a situation can be lawful and unethical at the same time. As has been pointed out, the legislation is some 20 years old, and technology moves at a breakneck pace.

Even with legal safeguards in place, can the use of these investigative tools become unethical?

[*English*]

Mr. Ronald J. Deibert: Thank you, Mr. Chairman.

I think the disclosure that there were warrants is certainly reassuring. I'm glad it's not the opposite case; however, I think that we need to put judicial oversight in the context of a number of different factors related to this environment—this topic that we're describing.

First of all, I think there is a problem with transparency and public accountability within our law enforcement agencies. In fact, there's a pattern, as my colleague Ms. McPhail said, of not disclosing ahead of time certain investigative techniques that require a public consultation. Again and again, these are coming out through media revelations or in a kind of backhanded way, and that's not the way to approach this topic.

Secondly, there's a—

The Chair: We're out of time for an answer. Maybe you can sum up in a few seconds, and then I'm going to have to go to Mr. Green.

Mr. Ronald J. Deibert: There are public safety issues with this very technology. There are equities involved because it involves exploiting flaws in software that make all of us insecure, rather than disclosing them to the vendors.

The Chair: Thank you.

Mr. Green, for up to six minutes.

Mr. Matthew Green (Hamilton Centre, NDP): I would love to continue along that line, because I think it's important for the benefit of this committee that we get a better sense of just what this sector looks like.

I know, Professor Deibert, you talked about its being rogue, mercenary companies. Can you perhaps expand on this, from your research, and what this sector looks like, who's acting in it, where the subject matter expertise is coming from and why we should be concerned about that?

Mr. Ronald J. Deibert: Very little is known about this industry; it operates in the shadows by definition. It's similar to the trade in weapons technology or private intelligence. These firms, generally speaking, don't like to publicly disclose what they're doing or who their clients are, which makes public accountability and transparency very difficult. We at the Citizen Lab, along with several other organizations, have spent well over 10, close to 15, years investigating this industry using a variety of technical methods and forensic methods.

What we've found is that there's almost no international regulation around this industry; they're selling to any government client. Most of the governments, unfortunately, in the world are authoritarian or illiberal, and naturally, they're using this technology not in the ways we're hoping for it to be used here. They're using it to go after political opposition, civil society, journalists, activists and others. They're making millions of dollars doing so, and they obfuscate their corporate infrastructure from investigators like us.

This is a very serious global human rights and national security issue. All you need to do is look at the reactions at the most senior levels of the United States government. The Biden White House, the Department of Justice, the Department of State and the U.S. Department of Commerce have all come out and said effectively exactly what I'm saying to you right now. We are really asleep at the wheel on the threats raised by the global mercenary spyware industry, and we need to urgently correct that.

● (1545)

Mr. Matthew Green: I know there's been local reporting, and we've heard it today, in testimony from the government side referencing a former prime minister, Stephen Harper, being involved. I think there are reports of a former ambassador to Israel also being involved, or at least reported as being involved. Can you speak to the relationship between those within governments who've had perhaps some of the highest levels of security clearance then acting as—and I think you framed it quite rightly—a "mercenary" sector? Can you talk about the dangers of people who have access to top clearances then retiring into this sector, both from elected and civil agencies, but also from some of our highest law enforcement agencies as well?

Mr. Ronald J. Deibert: This is a very serious concern, because there is a very well-documented revolving door, with people who work for intelligence services then going off and making money, some of them very honourably, unfortunately, and some of them not. I think it's shameful that a former prime minister would be involved in selling surveillance technologies, brokering Canadian firms' sales to Gulf clients who have a well-documented history of human rights abuses, which is why I said in my recommendations that we need to impose a lifetime ban on those who have worked for intelligence and law enforcement from ever working for mercenary spyware firms.

We also need to have clear rules in this country on export controls over surveillance technologies. Citizen Lab has documented the export of censorship and surveillance technologies made by firms based in Canada that have helped facilitate, frankly, violations of human rights abroad that would be unacceptable in this country. I'm shocked to say that there really are zero licensing or export controls in this country for the export or sale of spyware and surveillance technology of the type that we're talking about here. That needs to change.

Mr. Matthew Green: Just to be clear so that we can have you on the record, sir, is that a recommendation you're providing this committee so that we would recommend, as a committee, that these things be implemented, or is that just a comment?

Mr. Ronald J. Deibert: Yes, 100%, it was in my testimony as a specific recommendation. We desperately need guidance to Canadian businesses, clear ground rules on to whom they can sell their technology so that we don't end up having Canadian firms supplying surveillance technology like they have to regimes abroad such as the United Arab Emirates, Russia, Turkey and elsewhere around the world to help facilitate practices that would be clearly a violation of the charter in this country.

Mr. Matthew Green: There's still the concern that our government could do indirectly what it's not allowed to do directly by then taking advantage, perhaps, of information that might be unlawfully obtained by foreign actors. They could be friendly foreign actors; you can look at the use of Pegasus in places like Mexico. Pegasus is just a brand. It's the technology that's out there that's pervasive.

Mr. Ronald J. Deibert: That's correct.

Mr. Matthew Green: Could you comment, perhaps, on the possibility of having, in the hands of government, information that might be politically sensitive? We've seen this technology used against the media and against partisan opposition. Is that something you'd care to expand on and comment on here?

Mr. Ronald J. Deibert: Mr. Chairman, I would say that many of the manufacturers of spyware have close relationships, for geostrategic reasons, to the governments in the countries where they're located. I don't have any confidence that information that is collected by those spyware companies on behalf of government clients doesn't end up being passed on to specific individuals connected to their home government jurisdictions, which is why it's also a security risk.

We need to have better due diligence around procurement. With due respect to one of my fellow panellists here, I don't see any operational security reason that we cannot disclose from whom we're purchasing this technology. Disclosing that, frankly, has no bearing or tips off no one. It's good practice. It's mature, and a mature approach to a 21st century problem.

The Chair: Thank you.

With that, we will go to Mr. Williams for up to five minutes.

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

I'm going to stick to the professor as well.

Mr. Deibert, thank you for being here today.

In respect to the RCMP's use of this Pegasus-like cellphone hacking, this committee heard yesterday that these tools have been used since 2017, and not a single consultation has taken place with the Privacy Commissioner. They had to hear about it in the news. You understand well, as you've demonstrated, the implications this technology can have. Do you find the RCMP's decision to keep this information from Canadians acceptable?

● (1550)

Mr. Ronald J. Deibert: No, I don't find it acceptable at all, Mr. Chairman. I think that I heard something slightly different from the testimony. It sounded to me like one of the RCMP officers testified that they were using this type of technology much further back than 2017, which really is no surprise. As Ms. McPhail testified a few moments ago, there is a pattern of law enforcement agencies being reluctant, for whatever reason, to disclose what types of surveillance techniques they're using or specific technologies, hiding them from the public, and then somehow this information gets out, through media, ATIP requests or whatever, and they have to scramble to produce documents to justify *ex post facto* how they're using it.

Mr. Ryan Williams: One of the recommendations I feel we're going to have from this study is that all government agencies, no matter which they are, should have to complete or be mandated to lawfully complete a privacy impact assessment. Do you agree with that recommendation?

Mr. Ronald J. Deibert: Yes, 100%. It's the least that could be done, in my view.

Mr. Ryan Williams: Thank you.

Ms. McPhail, your organization has called ODIT the nuclear option for surveillance for the RCMP. Why do you refer to it as the nuclear option?

Ms. Brenda McPhail: Thank you for that question.

I think Professor Deibert has referred to this, but I'll elaborate.

We had yesterday an RCMP witness say, to paraphrase, that they don't actually think about doing a privacy impact assessment just because they're using a new technology. They consider whether the technology permits a new kind of invasion.

This sounds kind of logical until you break it down because that formulation of the nature of the search ignores the reality of an ODIT, which allows all the invasions all at once on a device that we— not they—own.

Did they do wiretaps before? Of course. Did those wiretaps allow access to the contents of every form of communication written and oral, professional and private, retrospectively and prospectively, including data that's not actually on the device itself but in the cloud? Of course not. Is it the same level of invasion? No. Did police install covert cameras in homes and places of business with warrants in the past? Of course. Did a single camera have the ability to move with an investigative subject from work to home, from bedroom to bathroom, 24 hours a day? Of course not. Is it the same level of invasion? No.

An ODIT can do more. It can record live audio. It can track locations. It collects device identifiers. It tracks Internet searches. It follows application use.

Should a PIA have been required? Of course. Even that, as Professor Deibert says, is not enough when we're talking about the enormity of the invasion.

Mr. Ryan Williams: Do you believe that, no matter who they are, any government agency using new technology should be required to do a privacy impact assessment?

Ms. Brenda McPhail: Any government agency wishing to use potentially rights-infringing surveillance technology that carries high risk to the public should absolutely have to do a mandatory privacy impact assessment, which should be made public in an appropriate form.

Mr. Ryan Williams: Thank you.

Mr. Juneau-Katsuya, in your work with government in the past or in your research, are any other agencies beside the RCMP using any technology similar to what we're investigating with the RCMP?

Mr. Michel Juneau-Katsuya: You would have to be a little bit more specific, but some of the technology of course—

Mr. Ryan Williams: I mean CSIS, CSE, anybody like that. Do you have any knowledge that any other government agencies besides the RCMP would be using Pegasus-like technology?

Mr. Michel Juneau-Katsuya: Other agencies are using it, probably, yes.

Mr. Ryan Williams: Thank you.

Mr. Chair, I think I'm out of time.

The Chair: You have about 15 seconds, so I don't know if—

The Chair: All right, that's what I like to hear. It keeps us on schedule.

With that, we'll go to Ms. Shanahan for up to five minutes.

Mr. Ryan Williams: I will cede my time.

Mrs. Brenda Shanahan (Châteauguay—Lacolle, Lib.): I'm sorry, Chair. I'm not ready to ask any questions.

The Chair: Oh, I hope I didn't get the order wrong.

Ms. Vandenbeld, go ahead please.

Ms. Anita Vandenbeld (Ottawa West—Nepean, Lib.): Thank you very much, Mr. Chair.

It's good to be back on this committee. The last time I was on the Standing Committee on Access to Information, Privacy and Ethics was for the Cambridge Analytica and Facebook study, and I found that we did some very good cross-partisan work on that issue.

This is, of course, an issue that concerns me very deeply. I'd like to direct my first question to Professor Deibert. As you know—and I think we're both on the World Movement for Democracy steering committee—I've long been an admirer of much of the work that Citizen Lab has been doing globally, both on disinformation and on cyber harassment of human rights activists. I think you've raised some very concerning points with regard to how authoritarian regimes are using these kinds of tools.

In terms of what this committee is looking at specifically, I know that some of the things you mentioned, particularly when you're talking about the digital transnational repression and other things, might more suitably be discussed at the foreign affairs committee or even the Subcommittee on International Human Rights, on which I sit. I think there would be significant interest in looking at that, including things like export controls.

My question for you is more specific. I think you'll agree that when the RCMP are using these tools in a very narrow scope—I think you mentioned things like “proportionate” and “necessary”—with judicial oversight and warrants, that's a very different thing than how regimes like China or Iran are using this kind of technology. Setting aside issues like the vendors and the export controls, you mentioned something that I think was interesting. You talked about having thresholds. Could elaborate a little bit about what those kinds of thresholds to prevent abuse of these kinds of powers would look like?

● (1555)

Mr. Ronald J. Deibert: I think overall it's reassuring that we heard testimony from the RCMP yesterday and from the minister that the instances of the use of this type of technology were undertaken with judicial authorization. However, as I said before, I think just because we hear from the RCMP that there was judicial authorization, it shouldn't be seen as some kind of magic wand that makes everything else magically disappear: “Nothing to see here. Go about your business.”

First of all, we know that there is a well-documented history of abuse within law enforcement in this country. There is a documented history of discriminatory practices. I also have concerns about the nature of the technology itself and whether, with all due respect to judges who I have confidence in, they truly understand the scope and scale and sophistication and power of the type of invasive technology we're talking about that Ms. McPhail just really accurately described.

I also think there are equities issues that need to be discussed here. My team and I routinely forensically analyze victims of spyware. In several instances, we've actually recovered copies of the spyware and made responsible disclosures to the vendors, unlike what the government agencies do. These disclosures have resulted in security patches affecting several billions of people worldwide. If the government is going to withhold that information from the vendors and put all of our safety at risk, there needs to be a proper process around that. That process typically is called the “vulnerabilities equities process”. Right now, as I said in my testimony, our process around that in this country is weak. It's opaque. Frankly, it's nowhere near the level of where it should be for a mature liberal democracy.

Those are some of the concerns I have that go well beyond whether the RCMP simply told us that these instances were authorized by a judge.

Ms. Anita Vandenbeld: Thank you. That's very helpful.

Mr. Juneau-Katsuya, I noted that you didn't finish the last part of your opening statement. I want to give you some time to do that now.

Mr. Michel Juneau-Katsuya: I thank you very, very much.

I want to bring to your attention the fact that, unfortunately, our society, particularly our democracy, is under siege. We're facing an enormous threat. Probably since the 1600s and 1700s, when the initial concept of democracy started to appear, we've never been under threat the way we are currently. The far right, the alternative right, is taking place. There's populist discourse. People are using demagoguery to try to convince people and bring insecurity.

From that perspective, I totally support the idea of bringing more control, more accountability and more transparency. What I seek is a balance, a balance that does not prevent the capability of also catching the bad guys. Unfortunately, all the nice discourses, theories and philosophical debates—they don't care about this.

● (1600)

The Chair: Thank you. We went quite a bit over there, but we got it all in.

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

[*Translation*]

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

Mr. Deibert, I have a limited amount of time, so I would appreciate it if you could keep your answer brief.

Are you in favour of having a third party examine the RCMP's activities in relation to surveillance tools?

[*English*]

Mr. Ronald J. Deibert: Yes. I'm in favour of as many legitimate parties as possible that are appropriate to make sure that we have proper accountability relative to the great leap forward in technological capabilities that law enforcement and security agencies have at their disposal today.

[*Translation*]

Mr. René Villemure: Thank you very much.

Mr. Juneau-Katsuya, at the tail end of a previous answer, you said that other agencies were probably using this technology.

Do you think that parliamentarians and elected officials have been put under surveillance by law enforcement agencies in the past?

Mr. Michel Juneau-Katsuya: Indeed, it has been necessary to surveil parliamentarians, because today, we have officials at every level, whether municipal, provincial or federal, who are in the pockets of foreign governments and are not necessarily working for Canada.

Those known as agents of influence are certainly out there. They can exercise influence, either consciously or unconsciously, but the result is the same from a national security standpoint and it puts Canada at risk.

Mr. René Villemure: Were tools like Pegasus used, or did that happen before?

Mr. Michel Juneau-Katsuya: It happened before and it's happening now. It's not something new. Foreign agencies have always tried to recruit elected officials. It's not that hard because politicians don't always listen to what the Canadian Security Intelligence Service, or CSIS, tells them or they simply disregard the information, because doing so is to their personal benefit.

Mr. René Villemure: Thank you very much.

Earlier, Mr. Deibert, you said that conducting a privacy impact assessment was the least that could be done.

What would be ideal?

[*English*]

Mr. Ronald J. Deibert: I think that we need to have some kind of embedded presence of the Office of the Privacy Commissioner. I was frankly very disappointed to hear that the Office of the Privacy Commissioner was not informed about these investigative techniques prior to the recent revelations, so we need to have a much stronger presence and, I would argue, even more capabilities and resources for privacy commissioners to act as a watchdog over our security agencies.

That's not to minimize the very important mission that law enforcement and other security agencies have in this country. We want them to be well equipped, but we need to have organizations that watch the watchers. In part, that's the mission of the Citizen Lab too. We act as a public watchdog.

The Chair: Thanks, Professor Deibert.

[*Translation*]

Mr. René Villemure: Thank you.

[*English*]

The Chair: We are over time with that.

Now, we'll go to Mr. Green for two and a half minutes.

Mr. Matthew Green: Thank you.

Ms. McPhail, you recommended that there be a civilian counterpoint to police applications for warrants within the judicial process. Could you expand on that, because it's something that I picked up as referring to what is a bit problematic in accountability throughout the warrants process.

Ms. Brenda McPhail: Absolutely.

This echos a recommendation that I made during the recent study on facial recognition technologies. It is that to counter this persistent pattern of police acquiring and using sophisticated and potentially controversial surveillance technologies without public disclosure, we should follow the lead of places like New York State and New Zealand in putting together an independent advisory panel that would include relevant stakeholders from the legal community, from government, from police and national security, from civil society and of course our regulatory bodies who are relevant, like the Privacy Commissioner.

It can act as a national standard setting body, an advisory body, to take a proactive look at the kinds of technologies that our police forces want to use to modernize their investigative techniques and look at them across a range of considerations, including ethical considerations, legal considerations and considerations around Canadian norms and values. It can then make standard setting, gold standard, recommendations for police organizations, not just nationally but provincially and territorially—because of course policing is also a provincial and territorial matter—so that we would have consistency and the public could be assured that rights were being respected while police had the tools they need to do their difficult jobs.

● (1605)

Mr. Matthew Green: Thank you.

The Council of Europe recognizes that the use of the Pegasus tool is a violation of article 8 on the right to privacy of the European Convention on Human Rights.

Does the Canadian legal framework guarantee privacy protections similar to article 8 of the European convention, such that the use of the device investigation tools with technological capabilities similar to Pegasus could be considered perhaps unlawful?

Ms. Brenda McPhail: I'm sorry. Is that for me?

Mr. Matthew Green: It was, yes.

Ms. Brenda McPhail: I think it's well known that Canada's privacy regime has fallen behind. I think that there have been many statements before this committee over the last almost decade documenting the ways in which our privacy laws for both public and private sector fall short and have gaps that fail to protect—

The Chair: Thank you, Ms. McPhail. We're over time.

Now we go to Mr. Hallan.

Welcome to the ethics committee and thank you for joining us today. You have the floor for five minutes.

Mr. Jasraj Singh Hallan (Calgary Forest Lawn, CPC): Thank you, Mr. Chair.

Thank you to the witnesses for being here.

Mr. Juneau, I want to pick up on something that you answered in response to my colleague, Mr. Williams. I found it very interesting that you said that other agencies are also using software similar to what Pegasus is. What other agencies are using these kinds of software and what are they doing with them?

Mr. Michel Juneau-Katsuya: Well, the agencies are the agencies are the national security agencies.

It's an investigative tool. They need to have it to be capable of pursuing some targets, some very dangerous and serious people. That is one of the tools that is accessible to them.

Mr. Jasraj Singh Hallan: What kind of software are they using? Is it the same software or is it different for each agency?

Mr. Michel Juneau-Katsuya: I do not have all the details of what kind of software it is or the name of the software at this point. I wouldn't be able to mention it.

Mr. Jasraj Singh Hallan: Is it different software for other agencies—you don't have to name them—or is it the same software being used by other agencies?

Mr. Michel Juneau-Katsuya: I don't have the details about which one the RCMP is using, so I'm not able to compare.

Mr. Jasraj Singh Hallan: In your opinion, is it just being used on Canadians or on foreign nationals also? Are they using the same software on foreign nationals?

Mr. Michel Juneau-Katsuya: To my knowledge, it's strictly on Canadians. Again, this has to be verified, as I'm not aware of all the operational uses.

Mr. Jasraj Singh Hallan: Has the use of the software, in your opinion, always been done with a warrant, or is some of this being done without warrants?

Mr. Michel Juneau-Katsuya: In my opinion, it's with a warrant.

Mr. Jasraj Singh Hallan: Is it every single time?

Mr. Michel Juneau-Katsuya: Again, I have not audited all of the agencies, so I'm not able to verify and certify that everything was done with a warrant. If I take an organization like CSIS, no investigation is done without due process of verification. Depending on what level of investigation is done, it might necessitate a warrant coming from a superior court.

Mr. Jasraj Singh Hallan: Regarding approval for a warrant coming from a superior court, is it one judge who's making a lot of the same decisions to grant that warrant? Have you seen different judges?

Mr. Michel Juneau-Katsuya: I've seen several judges in my experience. It's not always the same judge, but certain judges have been selected due to the national security and secrecy level.

Mr. Jasraj Singh Hallan: Okay, thank you.

Mr. Deibert, after watching yesterday's committee, you've seen what witnesses were saying. One issue that everyone is talking about right now is trust and how much it's been broken. You've brought it up, and many other people are talking about it.

After watching what the Minister of Public Safety said, how do you think Canadians can even trust some of our institutions today?

● (1610)

Mr. Ronald J. Deibert: We definitely have a problem of trust with public institutions, and we're not alone in that respect. Globally speaking, there's a decline around trust in public institutions, so we're not alone.

If we want to set a good example for the rest of the world and strive to be the best we can be, I think it's pretty simple that we can do better than what we have seen in this latest case which, as I've said before, follows a pattern of prior cases. First of all, we need to have a very clear public consultation in line with the magnitude of the technology we're talking about here, which represents a quantum leap forward in capabilities of surveillance.

Without that public consultation and trying to approach this subject in the ways that they have in the past, keeping it from the public and not disclosing things that could easily be disclosed, I think we're setting a bad example.

Mr. Jasraj Singh Hallan: I agree with you on that.

Mr. Juneau, you said that politicians on all levels have been monitored. We don't need to name names, but can you give us a number of how many, in your experience, have been monitored?

Mr. Michel Juneau-Katsuya: No, I cannot give a definite number considering the fact that in the concept of national security—

Mr. Jasraj Singh Hallan: Is it in the tens, the twenties or the hundreds? Can you give us something like that?

Mr. Michel Juneau-Katsuya: Again, it's difficult for me to mention the numbers because we work on a need-to-know basis. For example, if I have colleagues working on the Russia desk, they will not know if I'm working on the China desk and some of the targets I have.

What we know for sure is that we have various foreign countries that have succeeded in recruiting elected officials—municipal, provincial, or federal—and were capable of influence in this way.

We also see at the end of their mandate, cabinet ministers going to work for foreign companies that work directly against the national security and the national interests of Canada. There's a certain concern when some people leave public office, given what they have done during public office and what they do after holding public office.

Mr. Jasraj Singh Hallan: Okay. Thank you.

Mr.—

The Chair: You are well over time, but that was quite an extraordinary answer.

Mr. Jasraj Singh Hallan: Thank you, Mr. Chair.

The Chair: With that, I'm going to go to Ms. Khalid. Ms. Khalid will be last in the second round. Then we'll go to the next.

Go ahead, Ms. Khalid.

Ms. Iqra Khalid (Mississauga—Erin Mills, Lib.): Thank you very much, Chair.

Professor Deibert, one of my staff actually attended a number of your lectures as a professor at U of T, and he had some really good things to say about your role and expertise in this area. I really appreciate your being here today. Thank you very much. It's a personal connection.

I know members have been asking questions that you don't really have the purview to answer because you don't have the direct information. A lot of what we're discussing in this panel is, really, hypotheticals and what-ifs, with more of a policy perspective as opposed to a “what happened” or evidence-based perspective.

I'll start with Professor Deibert, if that's okay, and ask a question about disinformation.

We talk about the institutions that govern us and public trust. How does the concept that the RCMP and police institutions are monitoring and surveilling Canadians...? What kind of impact does that have? To date, we've heard from the RCMP and heard from the Privacy Commissioner with respect to exactly how many investigations have been conducted that have used ODIT surveillance. How does that impact public perception of the RCMP and our governing institutions in general, as we've seen the climate of disinformation and conspiracy theories being peddled in recent events? Professor Deibert, do you have any comments on that?

Mr. Ronald J. Deibert: Well, if I understand your question correctly, you're implying that there is disinformation about some of the concerns that are being raised with respect to the risks and threats of this particular industry, which our agencies are actually contributing to financially. I think you're very wrong. We have done well over a decade of evidence-based research, which has been cited widely, using technical means. We've verified hundreds of individuals worldwide who are neither criminals nor terrorists and who have had their phones hacked using this type of spyware by governments, both authoritarian and democratic. In one of the most recent cases, in Spain, we uncovered a massive surveillance espionage operation—

● (1615)

Ms. Iqra Khalid: I'm sorry to interrupt, but we're talking specifically about Canada. The scope of the motion and the study we have here is specifically about the RCMP. We're talking specifically about Canada, if you could limit your answers to that, please.

Mr. Ronald J. Deibert: Sure. As I said before, some of the remarks we heard in testimony from the RCMP were reassuring in terms of numbers and judicial authorization. I also heard, however, those numbers change in the course of a day. I heard that the Privacy Commissioner was not apprised of what's going on. I also heard the RCMP itself, in direct response to a question, say, “Yes, we undertake surveillance of Canadians”, which would be silly not to say because that's part of their job.

The issue is precisely the lack of transparency and public accountability. The way we're entering into this conversation is kind of backwards, frankly. This was disclosed, it seems to me, almost by accident, and we shouldn't be having a conversation like this about this important topic in such a manner. That's not disinformation. What we're dealing with here is a very important question. We need to be mature about it and talk about it forthrightly, rather than casting aspersions on people who are bringing up these important issues.

Ms. Iqra Khalid: Thank you for that, Professor Deibert. I appreciate it.

Monsieur Juneau-Katsuya, do you have any comments on that?

Mr. Michel Juneau-Katsuya: Well, I like very much, as I mentioned, the necessity to exercise control, accountability and transparency as much as possible. They are a cornerstone of our democracy. At the same time, we have a responsibility to work against and protect Canadians against some very serious threats that do not have any concerns about the philosophical debate of what is right and what is not right. They do it, period.

I'm absolutely and totally in favour of this capability to find the right balance, to question ourselves and to work constructively in allowing officers to be capable of performing their duties, while at the same time making sure, just as I said, that the end cannot justify the means. We have to be capable of striking that balance in order to be capable.

That also returns to the responsibilities of elected officials. Police are at the tail end of a problem. We're trying to resolve something when we are facing the problem. Sometimes the problem, like terrorism, emerges from the lack of actions taken by politicians earlier when the grievance was brought to their attention. It's not necessarily that you believe or you accept the grievance, but you must be capable of taking action. This is what the work of this committee is so important for.

The Chair: Thank you.

That concludes that five-minute spot. Now we're going to the third round. In accordance with the formula adopted by committee, first will be Mr. Bezan for five minutes.

Mr. James Bezan: Thank you, Mr. Chair.

Welcome to our witnesses. I didn't have a chance to ask questions earlier of Mr. Juneau-Katsuya.

Sir, I'm dumbfounded with what you just testified in saying that former politicians and politicians who are considered potential national security threats are being monitored.

In your experience as a former CSIS and RCMP officer, in those situations would jurisprudence be followed to ensure that their charter rights were protected by the issuing of warrants to wiretap or use spyware on those individuals?

Mr. Michel Juneau-Katsuya: To my knowledge, when a warrant was necessitated, yes, we used the warrant and the judiciary process was followed. Very often the politicians or elected officials, as I like to say, were not necessarily the initial target, but they actually came to our attention when we were watching foreign intelligence officers or foreign criminals or Canadian criminals being in contact with them. It became a concern to either CSIS or the the RCMP when these people demonstrated certain activities or certain actions that were questionable in light of the responsibility of their office.

● (1620)

Mr. James Bezan: In these situations, should I, as an elected official who has been very outspoken in my support for Ukraine, Taiwan, and other democracies that are under threat, be concerned that I may be spied on by Canadian federal agencies because of my advocacy for those countries?

Mr. Michel Juneau-Katsuya: No, but you're likely to be concerned about foreign entities spying on you or—

Mr. James Bezan: I always am. I just assume that.

Mr. Michel Juneau-Katsuya: That's why the RCMP exists, to try to protect you because of these positions that you're taking. This is what we enjoy in our society, this capability of having outspoken elected officials who speak on behalf of our community, just like you do.

Unfortunately, at the same time, you might become a target, and that's where we step in.

Mr. James Bezan: When we're looking at the overall use of technology—and I would say it's probably changed quite dramatically since you were working for CSIS—how do we ensure that it is being used for the correct applications? You said in your opening statement that you don't want this committee to get into the details and undermine operational capability, but at the same time, as you've said, we need to have transparency and accountability, and we need to know who is using this technology and how it's being applied.

Where is the counterpoint in this where it tips so that we're undermining the ability of our law enforcement agencies and national security agencies to protect Canadians?

Mr. Michel Juneau-Katsuya: I think some of the evidence and testimony presented by Professor Deibert and others is on the right track; that is, with regard to having certain entities that would be capable of doing the checks and balances, the verification, and asking for the accountability that is necessary. I think yesterday what I heard—maybe some people have heard differently—was the RCMP<s being open to this accountability. Maybe it didn't come soon enough or the transparency didn't come soon enough in the opinion of certain people, but this is what democracy in progress is about. This is something that needs to be constantly verified.

Having been an officer on the front line, I'm absolutely in favour of the capability of—

Mr. James Bezan: As an officer on the front line, can CSIS, as an intelligence agency, collect evidence that's not bound by the Canada Evidence Act or the Criminal Code? Can CSIS deploy this type of spyware without a warrant?

Mr. Michel Juneau-Katsuya: No. CSIS will usually have to go through a warrant process in order to collect this kind of sensitive evidence and use this kind of technology.

Mr. James Bezan: That's only if it's a Canadian. If it's a non-Canadian, they wouldn't be required to have a warrant?

Mr. Michel Juneau-Katsuya: No. If somebody represents a threat to national security, CSIS can go against a foreigner. For example, there are diplomats who are not diplomats. They are foreign spies. We go after them.

The Chair: That's it.

Now, we'll go to Ms. Vandenbeld. Go ahead for up to five minutes.

Ms. Anita Vandenbeld: Thank you very much.

I'd like to start my question with Ms. McPhail. When I was in graduate school I was on the board of the Alberta Civil Liberties Association, so I applaud the good work that you do.

When you gave your testimony, one of the things that you said at the very end was that there are more problems but also more solutions, and you didn't have time to outline all of them.

I think what this committee is very interested in are the solutions. Could you perhaps elaborate a little bit about what you see as some of the solutions and some of the ways in which the lawful, legitimate use of these kinds of technologies could be implemented without abuse and with proper accountability?

Ms. Brenda McPhail: I think there are a number of ways to proceed with legal reform across a range of different laws that would provide an improved baseline of accountability and transparency.

Previous witnesses yesterday talked about making privacy impact assessments mandatory, and I do support that recommendation as a baseline requirement. Also mentioned was the idea, which I support, of including the existence of privacy as a fundamental human right in both our public and private sector privacy laws. That changes the nature of the balancing act that's necessary when we're deciding whether businesses or governments are allowed to engage in invasive privacy practices. It puts the right at the centre, in a place where it should be in those balancing equations.

It's also worth looking at part VI of the Criminal Code, which, to the best of my knowledge, had its last very significant amendments slightly more than 20 years ago. It could be that experienced defence counsel in particular would be of great use to this committee in recommending alterations to that, based on their experience with these kinds of contemporary technologies as their use emerges in criminal cases.

Finally, as one more concrete thing, the United States has created an entity list of banned spyware vendors. Canada should absolutely consider doing the same thing, which would provide some public assurance that our tax dollars are not going to support these dangerous and mercenary companies.

● (1625)

Ms. Anita Vandenbeld: I appreciate that. Thank you very much.

My next question is for Monsieur Juneau-Katsuya. You mentioned in your testimony this need for balance. Certainly, we are all very much in favour of transparency, but you said in your testimony that even as we're here as a committee holding...to account, the bad actors are listening. I wonder if you could elaborate a little bit about how you achieve that balance while not providing information that could strengthen those bad actors.

Mr. Michel Juneau-Katsuya: I think we have mechanisms making us capable—sometimes in camera—of receiving and asking difficult questions. The House of Commons has established a permanent committee now on security and intelligence, which is capable of going across the board in every department to follow the traces of certain cases. That is extremely important.

The challenge that we have is that the sitting members are elected—just like members of this committee—and at every election there are new members who come in with a new team, a new group that doesn't necessarily have the experience, the knowledge or the network to be capable of digging in as much as they should.

Should we have more committees like the SIRC, the security and intelligence committee, which went from watchdog to lapdog over time? They're not really doing as much work as they should be sometimes to observe, criticize and bring solutions to some of the problems.

That's the problem: Sometimes the political systems interfere with the work of the committee and the independence.

You mentioned in one of your earlier comments that you enjoy the non-partisan element of the committee and the work that has been done. That's what should be sought as much as possible because, at the end of the day, we should be working for this nation, not for our partisan interests.

Ms. Anita Vandenbeld: I agree 100%.

How much time do I have left?

The Chair: You're down to 20 seconds.

Ms. Anita Vandenbeld: Thank you very much for that.

Mr. Michel Juneau-Katsuya: If I may add one element, we're spending a lot of time talking about law enforcement, which is the leitmotif of this discussion, but one area that has been neglected is the private world. Private companies are using this kind of technology far more than law enforcement, which is much more surveilled.

The Chair: Thank you.

We can only deal with so much within the constraints of a single, short study, but, indeed, we have heard repeatedly over and over again of the need for modernization of the Privacy Act, which would apply to private interests and corporations.

[*Translation*]

Over to you, Mr. Villemure, for two and a half minutes.

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

Ms. McPhail, do you think law enforcement's use of this kind of spyware violates the Canadian Charter of Rights and Freedoms?

● (1630)

[*English*]

Ms. Brenda McPhail: From what we've been told, in the way that these tools have been used, the RCMP has attempted to stay within the confines of the charter by ensuring that they get judicial authorization by using these for a small number of investigations and ensuring that it's only for crimes that are ostensibly particularly serious. The issue—

[*Translation*]

Mr. René Villemure: Sorry to cut you off, Ms. McPhail, but I have a limited amount of time.

Mr. Deibert, you mentioned in your research that Canada was this year's chair of the Freedom Online Coalition.

Would you say that, as chair, Canada has a duty to lead by example?

[*English*]

Mr. Ronald J. Deibert: Yes, I do.

[*Translation*]

Mr. René Villemure: What is the first thing you would recommend?

[*English*]

Mr. Ronald J. Deibert: Like I said, I think that we need to have, from senior officials, from the Prime Minister, from the Minister of Public Safety and from the Minister of Foreign Affairs, clear, forceful statements that this industry that we're touching on in this committee is a threat to human rights, democracy and to our own national security and that we are going to take measures aligned with our allies in the United States, Europe and elsewhere to start holding the worst actors in this industry more accountable and be more transparent and publicly accountable ourselves if we're going to use it domestically.

[*Translation*]

Mr. René Villemure: I gather that those at the top have to set the tone.

[*English*]

Mr. Ronald J. Deibert: Which we have not done, unfortunately, in contrast to the United States.

[*Translation*]

Mr. René Villemure: You're absolutely right.

Mr. Juneau-Katsuya, the revelation that elected officials can be recruited by foreign governments was troubling to me.

Can you provide the committee with a document or some observations to help us dig deeper into the issue?

Mr. Michel Juneau-Katsuya: I don't have any official documents. That analysis is based on the experience I've gained over the years.

For more specific information, you should reach out to the official agencies, mainly CSIS. In a television interview, former CSIS director Richard Fadden said that a number of elected officials at various levels of government had been compromised. I think the law enforcement agencies would have a lot of information on that.

Mr. René Villemure: Thank you very much.

[*English*]

The Chair: Thank you.

We have Mr. Green for two and a half minutes.

Mr. Matthew Green: Thank you very much.

Ms. McPhail, you mentioned part VI of the Criminal Code and the fact that it has been 20 years since it's been revisited. I think both you and Mr. Deibert have talked at length about the ways and the order of magnitude in which technology has far surpassed legislative guardrails or considerations. Part VI was cited at length and very frequently by both the minister responsible and the witnesses from the RCMP.

Can you comment from your perspective and opinion on ways in which you think, under the current legislation, the current laws in part VI, there remains a big gap in where we are now with these types of technological powers?

Ms. Brenda McPhail: Part VI of the Criminal Code—and I remind the committee that I'm not a lawyer, although I work for a legal advocacy organization—is generally written to be technologically neutral and to allow for the right kinds of inquiries to be made with the right safeguards, but, because the technology has changed so fundamentally my point was simply that those who are expert in the use of this part should ideally be allowed to comment on the ways in which it should be enhanced. I'm not the best person to comment on it; I simply wish to flag that it was a really important consideration.

Mr. Matthew Green: Yes. Is it a consideration that you would put as a recommendation from this committee that we recommend the government review part VI to ensure that it's in keeping with the advances in technology?

Ms. Brenda McPhail: Yes. That is my recommendation.

Mr. Matthew Green: Professor Deibert, is that one that you share as well?

Mr. Ronald J. Deibert: That's correct.

Mr. Matthew Green: I'll put the question to our last witness, whose name has escaped me; I apologize.

Is that something you would agree with, that part VI perhaps hasn't necessarily kept pace with technology and could, for the good and welfare of democracy and everything you've espoused in your testimony, provide that updated information and legal analysis?

Mr. Michel Juneau-Katsuya: It's a must.

Mr. Matthew Green: Okay.

Thank you.

The Chair: Thank you.

With that, we will move to Mr. Williams for up to five minutes.

Mr. Ryan Williams: Thank you very much.

Through you, Mr. Chair, this is to both Professor Deibert and Ms. McPhail.

Municipal and provincial police are not subject to the Privacy Act. Is that correct?

● (1635)

Ms. Brenda McPhail: Yes.

Mr. Ryan Williams: I'd ask both of you, with regard to recommendations to this committee, what parts of the Criminal Code should we be amending or making recommendations on to deal with these new techniques at this time?

Ms. Brenda McPhail: As we just discussed, part VI of the Criminal Code is the relevant section on electronic surveillance that requires a review.

Mr. Ryan Williams: Sorry. I meant to say as it regards provincial and municipal police forces as well and their use of this technology.

Ms. Brenda McPhail: Because policing is a provincial and territorial responsibility, there is actually a patchwork of different pieces of legislation that is relevant. That's part of an overarching problem in assuring that all police forces across the country adhere to golden, best standards when it comes to uses of surveillance technologies.

This is why, rather than doing a patchwork approach of encouraging provinces to amend a series of pieces of legislation in each of their jurisdictions, I recommend that there should be a federal advisory body to produce advisory bulletins, which those provinces can then take forward and attempt to implement within their own jurisdictions to achieve consistency and best practices across the country.

Mr. Ryan Williams: Thank you.

Professor, do you have anything to add to that?

Mr. Ronald J. Deibert: Yes. I would add that I am not a lawyer, but one thing I have observed from my research globally is that the spyware industry has a very strong appetite to sell to local law enforcement, where the abuses tend to be more problematic. Of course, they want to do this because it opens up new, prospective clients. I have great concern, beyond the RCMP, that there may be other agencies that have used these investigative techniques and we've not yet found out about them.

Mr. Ryan Williams: Mr. Juneau-Katsuya, you talked about this use of the current technology that we're talking about today being used in other government departments. I'm going to ask you specifically whether you know of other technologies. I mean, this technology we're talking about today was developed a decade ago. Are there new technologies?

I understand that you haven't been around some agencies for a little while, but do you know of any other technologies being used that this committee is not talking about today?

Mr. Michel Juneau-Katsuya: You would need to be a little bit more precise. For what purposes are—

Mr. Ryan Williams: I'll keep to the same theme, which is surveillance. I might be talking about drones or satellites. Are there other technologies that we're not speaking about today that you know are in existence?

Mr. Michel Juneau-Katsuya: Aerial surveillance from satellites, or coming now from drones, or from airplanes has been used for decades. What we do is to keep up as much as possible with the technology. Drones have now been used by other departments, particularly National Defence when it comes to the military theatre. There are other forms of surveillance done as well to track vehicles and track individuals other than with their cellphones.

So yes, a multitude of technologies have been used with the aim of being capable of mitigating the threats coming from the serious people we are tracking.

Mr. Ryan Williams: With some of those technologies, do you believe they're also being used by the RCMP? Would this be different government departments, or one or two?

Mr. Michel Juneau-Katsuya: When we talk about the surveillance element, what is also important is that not all surveillance equipment acquires information. Not all information is collected. Sometimes it's just to "tag" a person or vehicle or object in order to be capable of following the device that we are tagging.

So yes, other departments are also using surveillance techniques and surveillance technologies.

Mr. Ryan Williams: Regarding what we've talked about today, just to get your general perspective, do you believe we should be looking at privacy tools or making sure we're doing privacy impact assessments? With the technologies that come out, is there a role for the Privacy Commissioner?

Mr. Michel Juneau-Katsuya: Yes, there is a role for them.

Mr. Ryan Williams: Okay. Thank you.

The Chair: You're just about out of time.

Mr. Ryan Williams: I'm close enough.

The Chair: I'm going to go, then, to Ms. Hepfner for the final five-minute round.

Go ahead, Ms. Hepfner.

Ms. Lisa Hepfner: Thank you, Chair.

Mr. Juneau-Katsuya, I'd like to go back to you. You touched on your impression that revealing the source of the RCMP's spyware technology could render that technology unusable to the RCMP. Can you explain in more detail to this committee why that might be?

● (1640)

Mr. Michel Juneau-Katsuya: Well, contrary to Professor Deibert, I do believe—because we've done it ourselves—that when we are able to identify the technology that a foreign government or target is using, we are able to either use countermeasures or exploit that technology. The knowledge becomes intelligence. It becomes important now to know what the opponent is using in order to, as I said, counter or exploit.

That's why revealing it openly.... For this kind of technology, there's not a myriad of companies. There's a good number of them but there's not a myriad, so by isolating the country it's coming from and stuff like that, by deduction you're able to identify what the RCMP or any security agency is using, and therefore you're able to maybe mitigate their tactical capability.

Ms. Lisa Hepfner: Why do you think it's dangerous that at some points in this committee we've delved into accusations of mass surveillance or that unfounded suggestions of mass surveillance keep coming up? Why is that dangerous, coming from this committee, do you think?

Mr. Michel Juneau-Katsuya: There are two reasons. First of all, there's no evidence that there is mass surveillance. The other element is the cost.

One way to evaluate how possible or plausible it is that a technology has been deployed is to go with a cost analysis. Just one operation will easily reach half a million dollars. That's just to make one interception on one target with maybe one device only. It takes a lot of time and a lot of resources to install the software, monitor the software, debrief on the software and sometimes translate the language or the information that is there. When you add it up, at the end of the day there is a simple calculation of budget and we're not able to deploy that abundantly because it's too expensive.

Turning to what Mr. Snowden revealed of NSA capability, it's like talking apples and oranges. The NSA has budgets, capability and intentions that are way different from what the RCMP,CSIS or DND is capable of deploying here in Canada.

Ms. Lisa Hepfner: Thank you very much.

That's a perfect segue, Chair. With the last couple of minutes of my time, I would like to move a motion. The reason is that I think we have had a bit too much innuendo and too many accusations about mass surveillance at this committee, and even outlandish comparisons of the RCMP with the German Stasi. As a committee, we should come together and show support for the important work the RCMP does while ensuring their accountability under the Charter of Rights and Freedoms.

I will read my motion and we will circulate it to members of the committee in both languages as well. The motion reads:

> That the committee affirm that it is satisfied that the RCMP is not using Pegasus or NSO Group technology; that the use of ODITs is reserved for only the most serious cases; that the approval of a request to use ODITs comes with strict terms and conditions, and must be ultimately approved by a superior court judge; that the use of these tools without judicial authorization would be a criminal offence; and that the committee supports the RCMP in their mandate to protect Canadians from terrorism, human and drug trafficking, money laundering, and murder, while ensuring accountability.

I'm repeating myself here a bit. The final line reads:

> that the committee supports the RCMP in their mandate to protect Canadians from terrorism, human and drug trafficking, money laundering and murder, while ensuring accountability.

I apologize that in my copy I have it repeated, but we'll send the proper copy to all members of committee. I look forward to any questions my colleagues might have.

● (1645)

The Chair: Before we debate the motion, the clerk is just going to read the motion. Has it been received electronically? All right.

Mr. Matthew Green: Is there a speakers list here?

The Chair: No, I'm not quite there yet.

All right, thank you.

Thank you, Ms. Hepfner.

The motion is in order. I did have Mr. Green, and I also see Ms. Khalid next. Those are who I have for speakers so far.

Go ahead, Mr. Green.

Mr. Matthew Green: Thank you very much, Mr. Chair. I move to adjourn the meeting.

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

The Chair: I can't entertain a point of order if the—

Ms. Iqra Khalid: I had my hand raised before, right when Ms. Hepfner was reading the motion. I don't believe that anybody raised their hand before I had.

The Chair: I recognized Mr. Green. I can do my best to see who wishes to speak. Mr. Green was also trying to get my attention. In fact, I'm not even going to even rule on that point of order since we already had a motion to adjourn. With a motion—

Ms. Iqra Khalid: Sorry, Mr. Chair, I would like a ruling on that point of order. I feel that this is very unfair.

Mr. Matthew Green: He just did.

Ms. Iqra Khalid: I know that in the room I have been called out for not being there in person by members who have not shown up in person themselves for 75% of the meetings. I would appreciate it, Mr. Chair, if you could be a little more fair and judicious in how we conduct our meetings.

The Chair: Then we'll proceed. The clerk may proceed, then.

The vote is tied. I vote in favour of the motion to adjourn.

(Motion agreed to: yeas 6; nays 5 [*See Minutes of Proceedings*])

The Chair: The meeting is adjourned.