HOUSE OF COMMONS
CHAMBRE DES COMMUNES
CANADA

Standing Committee on Justice and Human Rights

JUST • NUMBER 027 • 2nd SESSION • 41st PARLIAMENT

EVIDENCE

Thursday, May 29, 2014

Chair

Mr. Mike Wallace

Standing Committee on Justice and Human Rights

Thursday, May 29, 2014

● (1100)

[*English*]

The Chair (Mr. Mike Wallace (Burlington, CPC)): Ladies and gentlemen, welcome to meeting number 27 of the Standing Committee on Justice and Human Rights. As per the orders of the day, we are pursuing our order of reference of Monday, April 28, 2014, for study of Bill C-13, an act to amend the Criminal Code, the Canada Evidence Act, the Competition Act, and the Mutual Legal Assistance in Criminal Matters Act.

We have a number of guests here today.

For the committee's information, I understand that there may be bells during this time. I have let the witnesses know that if there are bells, we will run over to vote and will come back to make sure that they get on the record with their 10 minutes.

Here is one other piece of information before we go on. I personally contacted Facebook and invited them to show either on Tuesday, which is when we have them scheduled, or Thursday of next week. We have not heard back whether they are taking us up on the invitation. We sent them copies of the motion from this committee from last time.

We were expecting Global News to be here, but they are not set up. As the rules state, there are no pictures once the gavel has been struck.

We are going to begin with our 10-minute presentations. We have the Canadian Centre for Child Protection with us today. We have the Office of the Federal Ombudsman for Victims of Crime. As an individual, Mr. Michael Geist is here. We also have the Canadian Association of University Teachers.

To make sure we move along quickly, let's have the Canadian Centre for Child Protection begin.

Ms. McDonald, you are taking the lead.

Ms. Lianna McDonald (Executive Director, Canadian Centre for Child Protection): Thank you.

Mr. Chairperson and distinguished members of this committee, I thank you very much for giving our agency the opportunity to provide a presentation on Bill C-13.

My name is Lianna McDonald, and I am the executive director of the Canadian Centre for Child Protection, a registered charity providing national programs and services related to the personal safety of all children.

Joining me today are my two colleagues: Ms. Signy Arnason, director of Cybertip.ca; and Monique St. Germain, our general counsel.

Our goal today is to provide insight and support for Bill C-13, legislation that will assist in addressing the non-consensual distribution of intimate images. We will offer some testimony based on our role in operating Cybertip.ca, Canada's national tip line to report the online sexual exploitation of children.

What we have witnessed first-hand and all too often is really the collision between sexual exploitation, technology, and bullying. For almost 30 years our agency has worked closely with families, police, educators, child welfare, industry, and others in child protection. Through operating Cybertip.ca, we have received more than 110,000 reports regarding sexual abuse and exploitation of children. These reports have resulted in police executing more than 550 arrests and removing numerous children from abusive environments.

It has been through this work that we see the most brutal behaviours towards children, everything from the recording of graphic sexual or physical assaults against very young children by predatory adults to teens trying to navigate a social media fallout from a sexual picture or even trying to cope with the aftermath of a sexual crime that has been recorded. These are not easy times to be a young person.

Several years ago we started to see a shift in reports to the tip line. We began to see young people coming in as both the victim and the reporting person. We recognized quickly the need to respond and as a result created a number of prevention resources. We have made these all available, and with a couple of samples that are very relevant to this particular issue.

While these and other resources are important, what we know is that they are not enough. Technology has become a powerful weapon and the ammunition of choice for those who wish to hide behind the protected cloak of anonymity. New technologies make it much easier to harass and to participate in a toxic digital frontier wherein ongoing biases about sexual misconduct collide with unrealistic expectations of adolescent behaviour, all fueled by the misuse of technology.

While certainly we are sophisticated enough not to place the blame solely on technology, we should be rightly committed to understanding its role in the commission of offences and to deciding how we as a nation choose to respond and modernize laws to adequately address new types of criminal behaviour.

The question we raise today is from a child protection point of view. How are we addressing the privacy rights of children? More to the point, how are we addressing the invasion of privacy of those young people who are currently being harmed? When young people are victimized and technology has been used to memorialize the sexual harm, there is often an additional layer of trauma. The past is their present.

For these reasons, we are supporting Bill C-13, and I want to highlight three key points.

First, we firmly believe that the intimate image offence is much more appropriate than a child pornography offence in circumstances in which both the individual depicted in the image and the individual distributing the image are under the age of 18. The child pornography offences were designed and intended to address behaviour and images that are qualitatively different from what we are discussing today.

Second, we support having the offence cover victims of all ages. Our agency receives reports and communications from numerous young adults impacted by this issue. The reputational and sexual harm that results from the non-consensual distribution of an intimate image is significant, regardless of age.

Third, it is important that such images be removed and deleted quickly to minimize the damage to the individual depicted.

We welcome the provisions in the bill that facilitate these actions. We also see tremendous value in enabling potential victims to apply for court-ordered recognizance against a potential distributor in advance of any distribution.

At this time, Signy Arnason, my colleague, will speak quickly to a few stats and facts, and then Monique St. Germain will speak to some criticisms of the bill.

● (1105)

Ms. Signy Arnason (Associate Executive Director, Canadian Centre for Child Protection): We would like to share with this committee statistics and facts from youth reporting to the tip line that informs our views on the issue of young people sharing sexual images and its impact.

Of the 110,000 reports that the tip line has received to date, 4% come in from a person under the age of 18. In the last few years, a number of these reports have been submitted from young people regarding self/peer exploitation and/or cyberbullying incidents. We also continue to receive a number of submissions into our "Contact Us" accounts.

The numerous examples we have received about the exchange of sexual images range from young people who voluntarily share a sexual image in the context of a relationship, youth who have been coerced into sharing a sexual image, and youth who have had an image taken without their knowledge.

Whether the information is submitted through Cybertip.ca or NeedHelpNow.ca, a site we specifically designed for youth, the number one request from those impacted by a sexual image being shared online is to get the content removed. These youth are desperate to get humiliating photos or videos of themselves off the Internet, and have had nowhere to turn to get the help they need.

NeedHelpNow.ca, in just over a year, has received 65,000 unique visitors, the most popular page being the steps you can take to remove content off the Internet. We believe the legislation will help address the dilemma for content networks when being asked to remove the content from their service. Such action can reduce the victimization of a young person significantly.

In the last year and a half we've had at least a dozen reports from youth either threatening self-harm or suicide in relation to the distribution of a sexual image. In one instance, we had to keep a family on the phone while we reached out to a mobile crisis unit.

We take every call, every "Contact Us" message, and every report very seriously; however, until there is legislation to address this issue, there is nothing to deter young people from engaging in this behaviour.

Ms. Monique St. Germain (General Counsel, Canadian Centre for Child Protection): We would also like to express some thoughts on a few of the criticisms that are being brought forward about this bill.

First, some are expressing concern that the bill will negatively impact youth and result in many more instances of youth being charged and jailed. As an organization dedicated to the protection of all children, we would prefer if this issue could be solved through prevention, education, and awareness. Unfortunately, there will be times when additional tools are required to deter the behaviour, address the harm, and protect current and future victims, who, in many cases, are also children.

What has not yet been mentioned is that if the accused is a young person, the Youth Criminal Justice Act will come into play. That act establishes unique, conceptual, procedural, and substantive safeguards that are specifically designed to protect the interests of young people. There are detailed provisions included within that act that mandate that each person involved with the young person, from police, to the crown, to the judge, must take into account the level of maturity and development of that young person, and consider alternative and restorative mechanisms throughout the entire process.

Secondly, there have been objections raised with this committee about the recklessness standard being too low. The recklessness standard was a specific recommendation of the CCSO cybercrime working group, in its report to the FPT ministers responsible for justice and public safety. We echo what was expressed by David Butt, from KINSA. The recklessness standard, in a criminal context, is not a carelessness standard. It is definitely the same as the law of negligence. We encourage the committee to ensure that any decision made on the issue of recklessness is based on a full appreciation of the way in which recklessness is applied in a criminal law context.

Thirdly, concerns have been raised that Bill C-13 unduly interferes with the rights of Canadians under section 8 of the charter. The bill has two important safeguards: the requirement to apply for a warrant, and judicial discretion to issue or not issue the warrant. Police have a duty to make full, frank, and fair disclosure of all material facts to the issuing judge when they apply for a warrant. In our view, a judge is in the best position to assess the request in the context of those facts. The only part of the bill that does not require a warrant is the preservation section, but preservation is not the same as production. In our view, this bill strikes the appropriate balance between privacy rights and the safety of Canadians.

● (1110)

Ms. Lianna McDonald: In closing, we know that the issues youth are facing today are far beyond what we might have imagined. We know that too many young people are suffering silently, and we have lost too many children to suicide, those who felt that there was no way out, no help, and no one who could make a difference. This is not acceptable.

No family is immune to this growing problem. The time is now to expeditiously resolve this debate. We understand that lawful access discussions have been going on for well over 10 years. From our agency's lens, there has been a serious price paid pertaining to the protection of children. While we welcome and appreciate the need for constructive debate, we are encouraging all parties to roll up their sleeves and find the necessary mutual ground, as children deserve no less.

Thank you.

The Chair: Thank you very much for that presentation from the Canadian Centre for Child Protection.

Our next speaker, whom we are all familiar with, is Ms. O'Sullivan from the Office of the Federal Ombudsman for Victims of Crime.

The floor is yours for 10 minutes.

Ms. Sue O'Sullivan (Federal Ombudsman for Victims of Crime, Office of the Federal Ombudsman for Victims of Crime): Thank you for inviting me here today to discuss Bill C-13, the protecting Canadians from online crime act.

I would like to begin by providing you with a quick overview of my office's mandate.

Created in 2007, the Office of the Federal Ombudsman for Victims of Crime receives and reviews complaints from victims, and promotes and facilitates access to federal programs and services for victims of crime by providing information and referrals. We promote the basic principles of justice for victims of crime, we raise awareness among criminal justice personnel and policy-makers about the needs and concerns of victims, and we identify systemic and emerging issues that may negatively impact victims of crime. Basically, we help victims of crime individually and collectively.

Bill C-13 covers a number of aspects relating to telecommunication and crime, including creating a new Criminal Code offence for the non-consensual distribution of intimate images, modernizing the Criminal Code, and providing new investigative tools for law enforcement. Given my mandate and our limited time today, I will restrict my comments to those sections of the bill that relate directly to victims, touching briefly on the importance of law enforcement's having the tools needed to prevent further victimization.

With that restriction in mind, I fully support the provisions of Bill C-13 that create a new offence related to the non-consensual distribution of intimate images, as well as the accompanying Criminal Code enhancements related to this offence, including: empowering a court to make a prohibition order limiting access of an offender to Internet or digital networks; empowering a court to order the removal of intimate images from the Internet; permitting the court to order forfeiture of the computer, cellphone, or other device used in the offences; providing reimbursement to victims for costs incurred in removing the intimate image from the Internet or elsewhere; and empowering the court to make an order to prevent someone from distributing intimate images.

This legislation, if passed, will help to provide tools necessary to assist in reducing cyberbullying and in providing victims with much-needed supports.

Cyberbullying is a relatively new but devastating issue. Canadians are struggling to find the best ways to understand it and most importantly to stop it. The problem of cyberbullying, as we have heard, is not a small one. In a 2007 survey of 13- to 15-year-olds, more than 70% reported having been bullied online, and 44% reported having bullied someone at least once. Canadian teachers have ranked cyberbullying as their issue of highest concern. Out of the six listed options, 89% said that bullying and violence are serious problems in our public schools.

I know you have had some witnesses come before you to discuss their personal and powerful experiences with cyberbullying. I would like to take a moment to acknowledge their bravery and leadership in coming forward to enrich this important public dialogue, despite how difficult it may have been for them. I have learned from speaking to victims directly that despite how hard it might be, victims come forward to discuss and advance these issues for the greater good, to ensure that others do not suffer the same pain they have suffered.

We know that any kind of bullying, including cyberbullying, can have serious and lasting impacts on victims. What is unique about cyberbullying is the staggering speed and reach of the abuse. In mere minutes, intimate or personal images can be shared across networks and the world, forever exposing their victims.

We also know that trying to contain an image that has “gone viral”, as they say, is no small feat, if not in some cases impossible. Even in situations in which victims work with professionals to remove the image, one can never be sure that someone somewhere doesn't have and won't recirculate these images. The feeling of being forever vulnerable and exposed and the long-term impact of the associated emotional burden that comes with it are something that we don't truly understand yet.

Technology and associated crimes are evolving faster than our ability to fully comprehend the lasting effects that these cases are having on victims. We know generally that victims of harassment report a loss of interest in school activities, more absenteeism, lower-quality schoolwork, lower grades, more dropping of classes, and truancy.

Addressing the issue can be equally overwhelming. For this reason, I support the bill's addition of “intimate images” to section 164.1 of the Criminal Code permitting a court to order the removal of intimate images from the Internet, as well as the element of the bill that empowers the court to make an order to prevent someone from distributing intimate images.

In cases in which an order has not been made, removing images is certainly not a straightforward task. For many, the thought of removing images from the Internet can be daunting. How does it work? How can I do it? Where do I turn for help?

In many cases, professional knowledge and service may be required in order to do it with any certainty or effectiveness. However, in cases in which private companies are engaged, there can be significant costs, and these costs should not be borne by the victims. It should never fall on a victim's shoulders to absorb the costs of removing images; that is simply unacceptable.

With that in mind, I support Bill C-13's proposal to provide reimbursement to victims for costs incurred in removing the intimate image from the Internet or elsewhere.

While I support these elements of the bill relating to restitution, I think there is a need first to extend the period for which restitution can be sought; second, to consider alternative supports for victims who cannot carry the upfront costs of image removal; and third, to build in or consider specifically how and when victims will receive information and guidance as to what options are available for removing images and when they can seek reimbursement.

● (1115)

It is my understanding that under the proposed legislation, restitution can only be sought for costs incurred up to the time of sentencing. This can be problematic for a few reasons.

One is that if the victim does not have sufficient funds to pay for the professionally assisted removal of an image themselves, then they may not pursue the option, given the risk that there may not be a conviction or that they may not successfully be reimbursed through restitution.

Second, even when a victim may be willing to take that risk, not all victims have the required funds available or own a credit card that they can use temporarily to cover the expense. In other words, if victims do not have the funds to cover the costs initially or the funds to cover the costs for a long enough period to receive a reimbursement, they will not be able to access the same level of service and protection as other victims, thereby creating an unfair balance in the system in terms of the supports offered to victims.

Finally, depending on the length of time it takes the victim to become aware of the option of professional assistance and/or the company to complete an invoice of work, it is likely that some expenses may be incurred only after sentencing. As I understand the bill, victim expenses occurring after sentencing would not be eligible for reimbursement.

While I support the intention of the bill, I would recommend that the committee consider amending this area of Bill C-13 to better meet the needs of all victims, no matter what their financial means, in terms of the support they may receive with respect to the removal of these images.

In cases in which a victim has the means and the option to pursue professionally assisted removal of images and subsequent restitution, ensuring that victims are provided with information concerning these rights and processes far enough in advance will be key. It is not clear to me how and at what point, if any, victims will be advised of their rights to seek a removal order or to file for restitution. I realize that these are details relating to implementation of the bill and that they may be addressed only at that stage; however, I feel it is important to note for members that without sufficient advance knowledge of these rights and options, victims may miss out on an important opportunity to address the damage done and to receive the supports they need and deserve.

Before concluding, I would like to touch briefly on what appear to be the most controversial aspects of the bill, those that relate to investigative tools and the balance of powers and privacy.

Privacy matters and technical investigative tools do not generally fall within my mandate. It is worth noting that among the victims we have spoken to there is no clear consensus on the elements of the bill. I have spoken with victims who very much support further measures to assist law enforcement in their investigation and who find the tools included in this bill to be balanced and necessary. I have also, like you, heard opposing points of view from victims who do not wish to see these elements of the bill proceed, for fear that they will impinge on Canadians' privacy rights.

From my own perspective I would say that there is a balance to be struck, and the dialogue that Canadians are having is a needed and valuable one. Law enforcement officials need the right tools at their disposal to quickly and effectively investigate these cases in order to help reduce cyberbullying in general as well as to protect potential victims. I believe there are some important tools in Bill C-13 to assist law enforcement in their investigation of these matters, and I support the proposed legislative changes that assist in ensuring that the data needed for investigation is preserved. Without it, there can be no evidentiary basis for important cases to proceed.

In conclusion, I support many aspects of Bill C-13 and commend the government for bringing to the table legislation that could assist in addressing cyberbullying incidents as well as provide victims with support in removing their intimate images from circulation. As stated, however, I would recommend that the provisions relating to restitution be amended to ensure that all victims, no matter their financial situation, be entitled to the same rights, opportunities, professional assistance, and reimbursement of costs, and that it be made clear how and when victims will be informed of their rights.

Thank you for your time.

[*Translation*]

Thank you.

● (1120)

[*English*]

The Chair: Thank you, Ms. O'Sullivan, for that presentation.

Our next presenter is a familiar face here on the Hill, Mr. Michael Geist. He is here as an individual, but he is the Canadian research chair for Internet and e-commerce law at the University of Ottawa.

Welcome back. You have 10 minutes, Mr. Geist.

Dr. Michael Geist (Canada Research Chair, Internet and E-commerce Law, University of Ottawa, As an Individual): Thank you, Mr. Chair.

Good morning. As you heard, my name is Michael Geist. I'm a law professor at the University of Ottawa. I have appeared many times before committees on digital policy issues, including privacy, but I appear today in a personal capacity, representing only my own views.

As you may know, I've been critical of the lawful access bills that have been introduced by both Liberal and Conservative governments. But I want to start by emphasizing that criticism of lawful access legislation does not mean opposition to ensuring that law enforcement agencies have the tools they need to address crime in the online environment.

As Ms. McDonald can attest, when her organization launched Project Cleanfeed Canada in 2006 I publicly supported that initiative, which targets child pornography by working to establish a system that protects children, safeguards free speech, and contains effective oversight.

In the context of Bill C-13 there is similar work to be done to ensure that we do not unduly and unnecessarily sacrifice our privacy in the name of fighting online harms. As Ms. O'Sullivan just stated, there is a balance to be struck, and as Carol Todd told this committee, we should not have to choose between our privacy and our safety.

Given the limited time, let me start by saying that I support previous witnesses' calls to split this bill so that cyberbullying can be effectively addressed in the way that we have just heard and that we can more effectively examine lawful access. Moreover, I support the calls we've heard for a comprehensive review of privacy and surveillance in Canada.

I'm happy to discuss these issues further during questions, but I want to focus my time on the privacy concerns associated with this bill. In doing so, I'll leave the cyberbullying provisions for others, such as those we've just heard, to discuss.

With respect to privacy, I want to focus on three issues: the immunity for voluntary disclosure provision; the low threshold for transmission data warrants; and the absence of reporting and disclosure requirements.

First is the creation of an immunity provision for voluntary disclosure of personal information. I believe this immunity provision must be viewed within the context of five facts. Firstly, the law already allows intermediaries to disclose personal information voluntarily as part of an investigation. That's the case for both PIPEDA and the Criminal Code.

Secondly, intermediaries disclose personal information on a voluntary basis without a warrant with shocking frequency. The recent revelation of 1.2 million requests to telecom companies for customer information in 2011 alone, affecting at least 750,000 user accounts, provides a hint of the privacy impact of voluntary disclosures.

Thirdly, disclosures involve more than just basic subscriber information. Indeed, this committee has heard testimony directly from law enforcement, in which the RCMP noted:

> Currently specific types of data such as transmission or tracking data may be obtained through voluntary disclosure by a third party....

In fact, since PIPEDA is so open-ended, content can also be disclosed voluntarily, so long as it does not involve an interception.

Fourthly, intermediaries do not notify users about their disclosures, keeping hundreds of thousands of Canadians in the dark. Contrary to some of the discussion we have heard, there is no notification requirement within the bill to address this issue.

Fifthly, this voluntary disclosure provision should also, I think, be viewed in concert with the lack of meaningful changes to Bill S-4, which would collectively expand the warrantless voluntary disclosure provisions to any organization.

Given this background, I would argue that the provision is a mistake and should be removed. It unquestionably increases the likelihood of voluntary disclosures at the very time that Canadians are increasingly concerned about such activity. Moreover, it does so with no reporting requirements, oversight, or transparency.

To those who argue that it merely codifies existing law, let me say that there are at least two notable changes, both of concern.

The first is that it expands the scope of “public officer” to include the likes of CSEC's and CSIS's employees and other public officials. In the post-Snowden environment, with global concerns about the lack of accountability for surveillance activities, this would run the risk of increasing those activities.

The second is that the Criminal Code currently includes a requirement of good faith and reasonableness on the part of the organization voluntarily disclosing the information. This new immunity provision does not include those requirements, potentially granting immunity even when disclosures are unreasonable.

In short, this provision isn't needed to combat cyberbullying; nor is it a provision in need of updating to combat cybercrime. In fact, I'd argue it is inconsistent with the government's claims of court oversight. I believe it should be removed from the bill.

The second issue I want to focus on is the low threshold for transmission data warrants. As you know, Bill C-13 contains a lower "reason to suspect" threshold for transmission data warrants, and as many have noted, the kind of information sought by transmission data warrants is more commonly referred to as metadata. Some have tried to argue that metadata is non-sensitive information, but that is simply not the case.

● (1125)

There has been some confusion at these hearings regarding how much metadata is included as transmission data. I want to state that this is far more than the question of who phoned whom for how long. It includes highly sensitive information relating to computer-to-computer links, as even law enforcement explained before this committee.

This form of metadata may not contain the content of the message, but its privacy import is very significant. Late last year, the Supreme Court of Canada ruled in R. v. Vu on the privacy importance of computer-generated metadata, noting:

> In the context of a criminal investigation, however, it can also enable investigators to access intimate details about a user's interests, habits, and identity, drawing on a record that the user created unwittingly....

Security officials have also commented on the importance of metadata.

General Michael Hayden, the former director of the NSA and of the CIA, has stated, "We kill people based on metadata."

Stewart Baker, the former NSA general counsel, has stated:

> Metadata absolutely tells you everything about somebody's life. If you have enough metadata, you don't really need content.

There are numerous studies that confirm Hayden's and Baker's comments. For example, some studies point to calls to religious organizations that allow for inferences about a person's religion, and calls to medical organizations that can allow for inferences on medical conditions. In fact, a recent U.S. court brief signed by some of the world's leading computer experts notes:

> Telephony metadata reveals private and sensitive information about people. It can reveal political affiliation, religious practices, and people's most intimate associations. It reveals who calls a suicide prevention hotline and who calls their elected official; who calls the local Tea Party office and who calls Planned Parenthood. The aggregation of telephony metadata—about a single person over time, about groups of people, or with other datasets—only intensifies the sensitivity of the information.

These are their comments—the comments of security experts in the area.

Further, the Privacy Commissioner of Canada has released a study on the privacy implications of IP addresses, noting how they can be used to develop a highly personal look at individuals.

Indeed, even the justice minister's report, which seems to serve as the policy basis for Bill C-13, recommends the creation of new investigative tools in which "the level of safeguards increases with the level of privacy interest involved".

Given the level of privacy interest that is involved with metadata, the approach in Bill C-13 for transmission data warrants should be amended by adopting the "reasonable grounds to believe" standard.

My third issue is transparency in reporting. The lack of transparency, disclosure, and reporting requirements associated with warrantless disclosures should be addressed. This combines both PIPEDA and lawful access, but it is made worse by Bill C-13. The stunning revelations we have seen about requests and disclosures of personal information—the majority without court oversight or warrant—point to an enormously troubling weakness in Canada's privacy laws.

Most Canadians have had no awareness of these disclosures and have been shocked to see how frequently they are used. The bills before Parliament seek or propose to expand their scope. In my view, this makes victims of us all, through disclosure of our personal information often without our awareness or explicit consent. When asked for greater transparency, such as we see in other countries, Canada's telecom companies have claimed that government rules prohibit it.

I hope the committee will amend the provisions that make warrantless disclosures more likely. But even if it doesn't, it should surely increase the level of transparency by mandating subscriber notifications, record-keeping of personal information requests, and regular release of transparency reports. These requirements could be added to Bill C-13 to lessen the concern associated with voluntary warrantless disclosure. Moreover, such reporting would not harm investigative activities and would hold the promise of enhancing public confidence in both law enforcement and communications providers.

Finally, I'd like to conclude, with all respect, by pointing to a personal incident involving one of the committee members, Mr. Dechert, that highlights the relevance of these issues.

Many will recall that several years ago Mr. Dechert was himself the victim of a privacy breach, with personal emails that were sent to journalists and were then widely reported in the media. This incident ties together several issues, which I have tried to highlight.

First, privacy interests arise even when you have nothing to hide and when you have done nothing wrong. The harm that arose in that case, despite no wrongdoing, demonstrates the potential victimization that can occur without proper privacy safeguards.

Second, much of that same information runs the risk of voluntary disclosure. Indeed, the expansion of the police officer definition means that in theory even political opponents could seek voluntary disclosure of such information and obtain immunity in doing so. Moreover, there is no notification in such instances.

● (1130)

Third and perhaps most important, the content of the emails that were disclosed was largely irrelevant. It was the metadata—who was being called or contacted, when they were being contacted, where they were being contacted, and for how long—that would itself allow for the same inferences that were mistakenly made during that incident. The privacy interest was in the metadata, which is why a low threshold is so inappropriate.

This kind of privacy harm can victimize anyone. As I've mentioned, we know that at least 750,000 Canadian user accounts are voluntarily disclosed every year—one every 27 seconds. It's why we need to ensure that the law has appropriate safeguards against the misuse of our personal information and why Bill C-13 should be amended.

The Chair: Thank you, Mr. Geist, for that presentation.

Next is our presenter from the Canadian Association of University Teachers, Mr. Turk.

The floor is yours for 10 minutes.

Mr. James L. Turk (Executive Director, Canadian Association of University Teachers): Thank you very much.

My name is James Turk. I'm the executive director of the Canadian Association of University Teachers. We represent 68,000 academic staff at 124 universities and colleges across Canada.

We've had a long concern with lawful access legislation as it has come through its various iterations. I would like to bring to your attention three concerns that we have with Bill C-13.

The first is, as Mr. Geist was mentioning, the reduction in the legal threshold to obtain personal records. The second is that Bill C-13 sets out that ISPs that preserve data or hand it over voluntarily will not incur civil or criminal liability. The third concern is that it adds “national...origin” to the definition of “identifiable group” in the Criminal Code. This is the part of the Criminal Code that relates to hate speech. It provides the possibility of criminalizing political discourse.

Let me deal with the first issue, and that is the lower threshold. Current Bill C-13 provisions for a production order for transmission data and tracking data reduce the threshold—as you know, I hope—from “reasonable grounds to believe” to “reasonable grounds to suspect”. This is a possible next step after a preservation demand or a preservation order for transmission data. The higher threshold—the current threshold—of “reasonable grounds to believe” still applies for production orders that exclude transmission data, so that if you want the content, the request has to meet the standard of “reasonable grounds to believe”. But if you want the metadata, it's only “reasonable grounds to suspect”.

Given the number of requests we know of in Canada in recent time, and given what we know of what is going in the United States.... You'll recall that in June 2013, the FISA court in the U.S. required Verizon to provide the NSA with all its customer metadata within the United States, including local phone calls. As a result, the NSA collected and retained all metadata for every call, every cellphone call, and every smartphone call attempted or made in the United States.

I agree with Mr. Geist that metadata can make the content irrelevant. The data crumbs that we use in communication technology, including the time and duration of the communication, the specific device that is used, and the geolocation, can allow enormous invasion of individuals' privacy rights.

Let's imagine that a member of this committee makes a telephone call to someone and then a week later visits an office building; sometime later makes a second phone call to a different number and a week after that, visits a different office building. What would the analysis of the metadata of this example look like or tell us? Well, if it is fed into a profile, the metadata on the telephone and the devices of the politician could tell a government agency that the first call was to a doctor; the first office building visited was a doctor's office. The second phone call was to a medical specialist; the second office building visit was to that specialist's office.

So what? We know that a politician has visited two doctors. All the government agency would then need to have access to is the Internet activity of that politician to have a very good idea what disease the politician was suffering from or was concerned about, if the member went on the Internet to WebMD.com/colorectal-cancer—or Parkinson's, or HIV.

Arguably, the metadata in the above example—two calls to two doctors, two visits to two separate doctors, and Internet activity in that time period—is as invasive as the content of communications. Bill C-13 lowers the threshold for state surveillance for that politician's visits to the doctors but maintains a higher level for any email message that politician might send to his or her spouse about his or her medical condition.

I can give you loads of other examples in which analysis of metadata can be highly invasive. Communication between a husband and wife can reveal many dynamics of their relationship: where they live, where they work, the time they go to sleep, when they wake up, when they leave home, and whether they're home together or not.

Access to metadata can also determine with reasonable probability that two people share a close relationship, by seeing that their devices are in the same location on repeated nights; or whether a person has a drinking problem from how often there are calls to Alcoholics Anonymous; or whether they are considering an abortion by knowing whether they have made calls to an abortion clinic; or whether they have a gambling problem, from their having made repeated calls to a bookie or to a helpline.

● (1135)

In other words, metadata are retained by an Internet service provider for a long period of time. The collection and analysis of these data in a large pool of metadata allow it to be matched up with real-world events. This makes it easier to get profiles and violate the privacy of individuals without the higher level of authority that would currently be needed in order to tap their telephone. A lower threshold of metadata opens the door to mass surveillance.

The second concern is the ISP immunity for turning over personal data. The Supreme Court, as you know, has reserved judgment on the constitutionality of the state obtaining subscriber information without a warrant under PIPEDA. We're expecting the decision in R. v. Spencer reasonably soon.

Advances in technology and the value of metadata for state surveillance make ISPs in many ways the gatekeepers of Canadians' privacy information. Offering civil or criminal liability exemption for ISPs invites ISPs to aid invasive state surveillance rather than incentivizing ISPs to protect Canadians' personal information with political and legal means. I would expect Telus, or Bell, or Rogers to have as their first interest protecting the confidentiality and the privacy of their subscribers' information. This bill would encourage them to see themselves as partners in state surveillance of their own customers.

The last comment is with regard to the expansion of hate speech to capture political speech. Bill C-13, as I mentioned at the beginning, adds “national...origin” to the definition of “identifiable group” in the Criminal Code. This part of the Criminal Code relates to hate speech. By including national origin as part of the definition of identifiable groups, certain speech—for example, speech critical of a national government, whether it be Israel, or Cuba, or the Ukraine—could be characterized as hate speech. We don't have to remember too far back, just to the 1980s, when a similar provision was used to prosecute persons critical of the apartheid regime in South Africa.

Like others who have appeared before this committee, we would encourage you to split the bill. Combatting cyberbullying is a worthy goal, but expanded surveillance powers over the citizenry by a government has the potential to represent an entire rebalancing between individual freedom and autonomy versus the power of the state. This fundamental tension in democratic society must be approached with care and an almost overabundance of consultation and concern for privacy.

Not doing so—refusing to split the bill and refusing to consider these concerns that Mr. Geist and I have raised—at best will represent for the Government of Canada an exercise in futility. Overreaching legislation will spend the next five to 10 years in the courts, and in our view, will be ultimately struck down as a violation of Canadians' constitutional rights. At worst, refusal to split the bill and revise these sections will increase government surveillance powers at the expense of individual liberty and autonomy, and Canadian citizens will be the worse for that.

Thank you very much.

● (1140)

The Chair: Thank you for those comments, Mr. Turk.

Now we move to the question and answer portion of today's meeting.

Our first questioner, from the New Democratic Party, is Madam Borg.

[*Translation*]

Ms. Charmaine Borg (Terrebonne—Blainville, NDP): Thank you very much.

I want to thank you for your testimony.

We have heard two different types of presentations. On the one hand, some witnesses talked about the part of the bill that pertains to cybercrime. On the other hand, some of them discussed provisions that may affect privacy. We feel this warrants a division of the bill, so that we can properly study those two aspects separately.

My first question is for Mr. Geist. Mr. Turk could perhaps also comment.

Both of you talked about granting legal immunity to telecommunications companies. We know that, in a single year, government agencies submitted 1.2 million requests to telecom companies. This bill would remove the risk of companies being prosecuted if they were to share certain information. This is a huge source of concern for me.

I would like to hear what you think about this. Could the fact that this bill removes that small legal responsibility increase the sharing of personal information without a warrant between the government and telecom companies?

[*English*]

The Chair: Mr. Geist, I think you were asked first, and then Mr. Turk can answer too.

Dr. Michael Geist: Thanks for the question.

I think there is enormous concern about the kinds of disclosure we've seen. I should note that even that number of 1.2 million probably doesn't fully reflect the number of requests that are out there. As you know, that was a request that came out of the Office of the Privacy Commissioner of Canada, and the telecom companies refused to provide individual responses. They got some to respond, and that information was provided in an aggregate manner.

I think it is striking to see the difference even between Canada and the United States with respect to the transparency associated with these kinds of activities. In the United States there are large telecom companies, such as Verizon and AT&T, that are now issuing transparency reports that are disclosing in an aggregate manner what's happening. From a Canadian perspective, we don't see the same thing happening with our own telecom companies. Some of them have argued that they are inhibited from doing so for legal reasons. I think that ought to be addressed.

Similarly, from an individual perspective, the lack of notification in these instances is enormously problematic. In many instances it's not clear that there is a legal restriction, a gag order. There has been in some other legislation. There is not necessarily under PIPEDA a gag order in many of these instances. What is simply happening is that there is a refusal or a decision not to disclose these kinds of requests.

I would argue that in sensitive law enforcement cases, law enforcement can get the necessary warrant and order to ensure that there is no disclosure where they think that will cause harm, but in other instances it's wholly appropriate for the telecom company, or whatever the intermediary happens to be, to notify the subscriber or their customer that their information has been disclosed.

The Chair: Mr. Turk.

Mr. James L. Turk: I share the view that the number of 1.2 million likely underestimates the requests.

Rather than just repeat what Mr. Geist is saying, because I'm in agreement with it, I think the police currently have the tools to do what they need to do. I think having the standard of reasonable grounds to believe as a condition of being able to get access to transmission data or content is a reasonable standard and should be maintained.

I am also deeply concerned about the apparent lesser transparency in Canada than in the United States and the lesser sense of responsibility of protecting their customers that Canadian Internet service providers seem to have. This bill will only worsen that situation.

● (1145)

[*Translation*]

Ms. Charmaine Borg: Thank you.

We see that the lack of transparency seems to be a major issue. I agree that this 1.2 million figure was achieved even without all telecom companies answering the commissioner's question. In the absence of that question, we would have never known what the situation was, and that is very problematic.

When we debate these issues in the House of Commons, we are always being told that this information can be found in a phone book. However, that is completely false. An IP address can reveal a great deal about an individual, just as metadata can.

Mr. Geist, you gave us some idea of what an IP address is and what it can reveal about an individual. Can you elaborate on that?

[*English*]

Dr. Michael Geist: With respect to the specific question on what is an IP address, in some ways it's our location on the Internet. That same IP address can disclose—and I commend the Privacy Commissioner's report on this—more than just the computer or the device we happen to be using, because that information gets placed in many places all around the Internet. For example, if you're involved in a Wikipedia edit, your IP address is logged and becomes publicly available. There is the ability to use even that kind of information to begin to develop a profile of someone's activity online.

You highlighted it, but I think it's worth emphasizing that under PIPEDA the exception for law enforcement as currently structured today is by no means limited to basic subscriber information. This notion gets propagated again and again, and I'm sorry but it's simply false. The opening is to allow for disclosure, full stop. In fact at this committee you heard from the RCMP that it includes transmission and tracking data, but frankly, it could in theory include content as well from an intermediary who has it, if it's part of a lawful investigation.

[*Translation*]

Ms. Charmaine Borg: Thank you very much.

[*English*]

The Chair: Now I'll go to Mr. Dechert, our first questioner from the Conservative Party.

Mr. Bob Dechert (Mississauga—Erindale, CPC): Thank you, Mr. Chair.

Thanks to each of our witnesses for being here today.

Mr. Geist, I'd like to respond to you. You mentioned something that occurred with respect to messages between me and another party, which were stolen by a third party and publicized. Some of my friends in the media had some fun with that issue.

But what this bill, sir, is about is protecting kids from Internet crime. I'm an adult. I'm a lawyer. I'm an elected official. I've been sent here twice by thousands of people in my riding to represent them, and I'm still sitting here, talking to you today, unlike Rehtaeh Parsons or Amanda Todd or Jamie Hubley. That's the difference. I didn't suffer. Sure there was some embarrassment, but I'm telling you, I didn't suffer.

If I had suffered, I had ways to address that. I could have sued the individual. I could have sued the media. I know how to do that. I am confident that the people in my riding support me, but I am here talking to you, and there are other people who are not. What we need to do is to give law enforcement the tools to protect the people who can't protect themselves.

I'd like to turn to Ms. O'Sullivan—

A voice: [*Inaudible—Editor*]

The Chair: It's his time, Mr. Geist. He can do what he wants.

The bells are ringing, so I'm going to suspend the meeting. We'll stop the time here for you, Mr. Dechert. We will be back after this vote and then we will continue with the questions and answers. We're going to try to make sure we get in at least one round.

The meeting is suspended.

● _____ (Pause) _____ ●

● (1235)

The Chair: I call the meeting back to order.

I appreciate the patience of our witnesses. We've had the vote and we're back. We should be able to get the first round in, so every party will have an opportunity.

Mr. Dechert, the floor is still yours.

Mr. Bob Dechert: Thank you, Mr. Chair.

Ms. O'Sullivan, when we broke, I was about to ask you about striking the right balance between addressing the needs and concerns of victims, while also protecting civil liberties. As you know, we're all struggling with this here. Where do you draw the line between the release of what some people, some civil libertarians, may say is private information and being able to work quickly enough to save the lives of vulnerable people?

On Tuesday at this committee we heard from Mr. Gilhooly, who is both a lawyer and a victim himself. He is a brave man, and he has come forward to tell his story about how he was victimized by Graham James.

I asked him that same question, and he said, “my hope is that we're going to err on the side of giving the police the appropriate tools to intervene”, and that in instances in Bill C-13 where there is no egregious violation of privacy rights that comes into play, “We, as victims...don't want to see rights trampled, but the tie has to go to the victim here”. Let me go on for just a minute also because I want you to know what the other side said. The Criminal Lawyers' Association said that a “tie doesn't go to the victim”. It said, “The tie should go to the charter, which is the supreme law”.

Would you agree that the government has a difficult task in finding the right balance between civil liberties and the protection of Canadians and victims? Would you agree that instances where there is no egregious violation of privacy rights, the tie must go to the victim? What's your view on that?

● (1240)

Ms. Sue O'Sullivan: I'd like to start with the comment that, first of all, I think it's so necessary that we respect all the opinions that are involved in this conversation and the need, as you say, to strike that balance. I'd also like to acknowledge particularly that there have been many victims' families, particularly on the cyber issue, who have spoken quite publicly about their leadership, about their bravery, and about their leadership in terms of ensuring that we in this country have this conversation—this very important conversation—about that balance.

This conversation is not unique to this bill. This is something that we constantly have to be looking at, but in my opinion, the tools that are in this bill are needed to ensure that law enforcement can conduct that investigation. My understanding is simply that there is information that comes in specific to an investigation. They then ask the telecom provider to preserve that information and they then get judicial authorization to access that information. So I think that does.... I mean, when you talk about checks and balances, I certainly think that judicial authorization is an appropriate check and balance.

So as we move forward—and I did in my comments talk about technology and its impact—this won't be the end of these conversations. It is a conversation that I think not just parliamentarians and governments continue to have, but that Canadians need to have, because it is involving us in that very public discussion that allows us, as Canadians, to really ensure.... In a way, it's another method of oversight that Canadians are having this very important conversation. But in my opinion, these tools are needed to assist law enforcement in ensuring that we have the ability to gather and preserve that evidence.

Mr. Bob Dechert: Ms. McDonald, what's your response?

Ms. Lianna McDonald: Well, as I think as we stated at the outset, we certainly believe that this bill finds that right balance. From our agency's perspective, we've relied heavily on looking at what has been put forward. We have a very thorough report from the CCSO cybercrime working group. It's our understanding that there have been years of consultations on this issue, so we have had a lot of the right stakeholders around the table over the years, working through some of these sensitive areas. Again, we believe that this bill finds that right balance and it's time to take some action.

Mr. Bob Dechert: Have I more time? Okay.

I have a quick point for Ms. O'Sullivan. You were formerly a police officer.

Ms. Sue O'Sullivan: Yes, I was.

Mr. Bob Dechert: One of the comments that's been made about this bill is that the person whose information is being disclosed should be notified at the time the request is made. As a police officer, what do you think would happen to that data if that were to happen? Would it be destroyed? Would it be deleted?

Ms. Sue O'Sullivan: First of all, I have been out of policing for five years, and I know that you had an expert panel of law enforcement here, so I would certainly defer to law enforcement to speak to the specifics of that. It is really within their purview, but at the end of the day, I think the right questions are being asked. As I say, I know that Chief Chu and several from senior law enforcement were speaking to that.

Mr. Bob Dechert: Thank you.

The Chair: Thank you very much.

Now, from the Liberal Party, we have Mr. Casey.

Mr. Sean Casey (Charlottetown, Lib.): Thank you, Chair.

Mr. Geist, in the opening of his round of questioning Mr. Dechert took quite a rip at you, and you didn't get a chance to respond. You can use some of my seven minutes to do that if you wish.

Dr. Michael Geist: Thanks for that.

My only response was going to be that we're in agreement. We both agree victims, especially in the cyberbullying context, need to have recourse and need to have appropriate tools.

My only point in raising the issue was that victims of privacy breaches are of all ages and from all different walks of life. In fact in many instances these happen while people are blissfully unaware of what is taking place.

I would argue that, in the context of this bill, given that cyberbullying contains what is very clearly a significant privacy element, we shouldn't be killing privacy in order to save it, from a cyberbullying perspective. There are better ways to address what at the end of the day are a couple of very specific kinds of concerns at a time when frankly there's a fair amount of agreement on a lot of the provisions found in the bill.

● (1245)

Mr. Sean Casey: Thank you.

I want to focus in on the non-consensual distribution of customer information with immunity and without a warrant. Several of you have addressed it.

Mr. Geist, a couple of things you said in your opening statement were about the telephone companies, and if I can, I want to drill down a little bit on that. One of the things you said, with respect to transparency reports, was that telephone companies indicate there are actually some government rules that prohibit that.

We heard from the minister on this topic. I asked him directly about transparency reports or the provision of information by telcos regarding how often they are disclosing information without consent and without a warrant, and whether they have an obligation to talk to their customers about it. The answer I got was that it's contractual between the customer and the telco.

I'd like you, if you would, to help me understand this. If the telcos are saying the government prevents them from providing greater transparency, and the government is saying that's between them and their customer, what are we to believe, and where do we go?

Dr. Michael Geist: I think we need to do a couple of things. Earlier this year all the major telcos were asked in a letter sent out by many in the privacy community in Canada to disclose some of their practices. We need to recognize that they all declined to do so citing Solicitor General rules, and generally saying that if the government told them to make these kinds of transparency disclosures they would, but otherwise they felt inhibited from doing so even on an aggregate basis.

Their current position is that they are not moving forward with that. We could have the government say it thinks this kind of aggregated information is important even on an aggregate basis. I'd note that, even with respect to individuals, Mr. Dechert, in his last question suggested that somehow those seeking notification are looking for immediate notification as law enforcement is actively engaged in its investigation. I do not believe that's what I said or what many other people have said.

We have said that a customer ought to have the right at some point in time to be notified if their information has been disclosed—deciding when an appropriate time would be is, I think, a matter of some importance and some debate—but I haven't heard anybody suggest there should be a disclosure to that underlying customer if it would cause or imperil the investigation itself.

Mr. Sean Casey: Several of you talked about immunity, and that's been the subject of much conversation in other committee hearings as well. I don't know if you're going to be able to help me with this. This question is for Mr. Geist and for Mr. Turk as well.

Why is it there? Was it at the behest of the telephone companies? What motivated the insertion of the immunity—especially when the government says that it doesn't mean anything and that it was already there—into this bill? I'd like to hear from both of you on that, please.

Mr. James L. Turk: I don't know the motivation behind it. I suspect the primary interest of the telcos and Internet service providers is that it may pre-empt class action suits against them. They have relatively little vulnerability.

I think a more important aspect of its inclusion, which I tried to address, is that it essentially offers an incentive for the ISPs to think of their relationship with the government, not of their obligations to their subscribers.

Dr. Michael Geist: Sure, and I certainly agree with what Mr. Turk had to say. I think it likely is that potential liability coming around to class action, but at the same time, I would suggest that if we take a look in totality around the privacy policy issues, both with this bill and with Bill S-4, those actually suggest that the government is promoting and pushing towards more voluntary warrantless disclosure. We see it with an expansion of that kind of provision within Bill S-4, and we see it here now providing immunity regarding the disclosures that do take place.

What it does is send a signal, I think, to those who collect information, telecom companies and others, that we are going to create and we are moving towards a framework that will encourage that voluntary cooperation, that voluntary disclosure, without the courts.

We've heard, I think consistently, from other members on the panel that this bill is striking the right balance. They say that consistently with the proviso that the court is involved. Let's recognize that, in these circumstances, the court is not involved when these voluntary disclosures take place.

● (1250)

The Chair: That's your time, Mr. Casey. Thank you very much.

Our next questioner from the Conservative Party is Mr. Seeback.

Mr. Kyle Seeback (Brampton West, CPC): Thank you, Mr. Chair.

I'll try to move quickly. I have very limited time.

Ms. St. Germain, I think you talked about the recklessness standard. We had another witness come on Tuesday, Mr. Butt, and here's what he said at committee:

> At the risk of oversimplifying this, it is not carelessness. Carelessness is inadvertent conduct. You don't even turn your mind to the risk. Recklessness is you turn your mind to the risk and you go ahead anyway. How can it be wrong to say to even a teenager, you turned your mind to the risk that you were distributing somebody's inappropriate intimate images, and you went ahead anyway.

I take it you would agree with the assessment he made on Tuesday.

Ms. Monique St. Germain: The recklessness standard, when it's interpreted in a criminal context, involves a subjective element. The person who commits the offence has to actually recognize that there's a risk in what they're doing, which is a little bit different from just being careless. That's a much lesser standard, so yes.

Mr. Kyle Seeback: You would agree, then, with what he had to say in his analysis.

Ms. Monique St. Germain: Yes.

Mr. Kyle Seeback: Great. Thank you.

Mr. Turk, I want to talk to you about your concern with respect to the standard of reasonable grounds to suspect versus reasonable grounds to believe with respect to transmission data. We keep hearing that this is about metadata, and I'm going to respectfully disagree. I think transmission data is a narrower category of metadata. You get less information than you would with metadata, with transmission data.

You're saying that this is lowering the standard. In other circumstances, it's the reasonable grounds to believe. But if you want to get a telephone recorder, which will give you the information of where a phone call originated from, who the phone call went to, and how long the phone call took place, that's subsection 492.2(1) of the Criminal Code, and to get that, it is reasonable grounds to suspect.

So it's not lowering the standard. In fact it's the same standard. People are saying, as you are saying, that the big problem is that on an email you can find out that they emailed a doctor, and therefore you're getting personal information, and that should be at a higher standard. Well, you get that from a phone call too. All you have to do is look up on Canada 411 what that phone number was.

So actually the standard isn't changing. It's the exact same.

Mr. James L. Turk: I think you're the first person I've run into who has suggested that the kind of information one can get from land-line phone records is equivalent to what one gets through Internet metadata.

Mr. Kyle Seeback: But it's not metadata. It's—

Mr. James L. Turk: Well—

Mr. Kyle Seeback: What you get from transmission data is the type, date, time, origin, destination, or termination of the communication. It does not include the content. What you get from a telephone is the time, the date, the origin, and where it went to.

I'm not seeing the gigantic difference that requires a higher level of proof, because you still have to get judicial authorization even on reasonable grounds to suspect. They have to go before a judge and convince a judge that they suspect a crime was committed before they get transmission data.

Mr. James L. Turk: All of the legal experts I know feel that there's a significant difference between reasonable grounds to believe and reasonable grounds to suspect.

Mr. Kyle Seeback: There is. Correct.

Mr. James L. Turk: That's first. Second, I tried to give some examples of cases, using you as an illustration, as to the kinds of information that can be compiled under this provision that would reveal a good deal of personal information.

Mr. Kyle Seeback: You suggested that I sent an email to a doctor, right?

Mr. James L. Turk: Yes.

Mr. Kyle Seeback: Then, after I sent another email to another doctor, they figured out that I went to see a colon cancer specialist or whatever.

Can you not get that exact same information from the telephone calls that I would have made to those people, that I called two different doctors?

● (1255)

Mr. James L. Turk: It's the combination of who you contacted, when you contacted, and what other Internet activity you had in relation to it, in that time period, that can be assembled; that is what's so revealing. You can't do that just from—

Mr. Kyle Seeback: With judicial authorization, so the police—

Mr. James L. Turk: At a level of reasonable grounds to suspect....

I mean, look, if indeed the police have reasonable grounds to believe, that's not an impossible standard, so why lower it?

Mr. Kyle Seeback: It's not lowered. Because if you're getting that information from a telephone call—

Mr. James L. Turk: It is. If it's not lowered, then why aren't you prepared to have reasonable grounds to believe as the standard?

Mr. Kyle Seeback: So we should change it for telephone numbers as well.

Mr. James L. Turk: Yes.

Mr. Kyle Seeback: It should be reasonable grounds to believe; so you're saying change subsection 492.2(1).

Mr. James L. Turk: If you're using that as the justification for this, then yes, change that.

The Chair: You have one more minute.

Mr. Kyle Seeback: The argument I think I keep hearing from people like you is that you're suggesting that the police will go before a judge—because they have to go before a judge, right?—to obtain this court order and convince a judge, on reasonable grounds to suspect that a crime occurred, that somehow they will—

Mr. James L. Turk: Or it will occur.

Mr. Kyle Seeback: —or will occur, and will somehow use that to get information on average Canadians. So the police just have the time to run around, go to a judge, having gone through the chain of command to be able to get the authority to go to a judge just to get information on random Canadians. That's the concern.

The Chair: Please give a relatively succinct answer.

Mr. James L. Turk: I'm not making a comment nor attempting to impugn police. We set our law and we set standards based on what we think is appropriate. We're not attributing motivation. The judge has to live within those standards, and we're saying there should be a fairly high standard before this kind of information can be released.

The Chair: Okay. Thank for you that. That's your time.

We have about two minutes left. It's the New Democratic Party's turn.

So, Madame Boivin, I'm going to cut you off within two minutes.

[*Translation*]

Ms. Françoise Boivin (Gatineau, NDP): Okay, I will try to be quick. That's too bad, since this group of witnesses is extremely interesting. I would have liked to ask each of them some questions.

[*English*]

We talked about notification. I think it's important to remove some of the innuendoes that I kind of heard from the government side. Nobody is asking to have the police or the provider notify the person who is under investigation at that moment.

Am I correct in thinking it's more in the sense of

[*Translation*]

wiretapping, for instance? Would those be the kinds of cases where a request would be made for reports, for people to be informed within a certain timeframe, following investigations, and so on? Is that what is meant mean by notification?

[*English*]

Dr. Michael Geist: The issue that I think a lot of people have raised is both in the context of the bill and also in the context of the revelation of there being over a million requests for this information. So while Mr. Turk has asked whether people are phishing and stuff like that, I'm not accusing people of phishing, but I know there are requests for 750,000 user accounts to be disclosed on an annual basis. That's a whole lot of people's information that's being disclosed—

Ms. Françoise Boivin: And it's not unreasonable—

Dr. Michael Geist: —and all the providers, every single one, said that they did not notify those disclosures to the underlying customer.

Ms. Françoise Boivin: And it wouldn't be unreasonable to notify these people, “Listen, your information has been provided”. That's one question I had.

The other one that we didn't have time to touch on with you guys and I think is important is the

[*Translation*]

definition of the terms “peace officer” and “public officer”. The definition of “public officer” is provided a few paragraphs above the proposed clause 487.012. As for the term “peace officer”, it is defined in section 2 of the Criminal Code, but the fact that the definition is very long worries me a little.

Do you think legislators should narrow the definition that determines who has the power to do what is set out in these provisions?

[*English*]

The Chair: Mr. Geist, my suggestion is that you provide through the clerk your answer to that particular question on the definition of a peace officer. Thank you very much.

I want to thank our panellists for coming.

Just so you know, we have one more week, next Tuesday and Thursday, of witnesses on this particular topic, on this bill. Then for the week after, the Tuesday and Thursday, the plan is to be going clause by clause, with any anticipated amendments. If you have any suggestions for our colleagues on either side of the House for amendments you'd like to see, please pass those along and we'll be dealing with them.

Thank you very much for this excellent panel, and I do apologize for the disruption with the vote.

With that, we are adjourned.