HOUSE OF COMMONS
CHAMBRE DES COMMUNES
CANADA

Standing Committee on Justice and Human Rights

JUST • NUMBER 021 • 2nd SESSION • 41st PARLIAMENT

EVIDENCE

Thursday, May 1, 2014

Chair

Mr. Mike Wallace

Standing Committee on Justice and Human Rights

Thursday, May 1, 2014

● (1140)

[*English*]

The Chair (Mr. Mike Wallace (Burlington, CPC)): I'll call to order this meeting of the Standing Committee on Justice and Human Rights. This is meeting 21, and it's Thursday, May 1.

Before we move to the orders of the day, we have the third report from the subcommittee from last Tuesday, which authorizes two things: one, that the Minister of Justice come next Thursday, May 8, for our main estimates, and second, for the beginning of today's study on Bill C-13.

Can I get a motion to approve that?

An hon. member: I so move, Chair.

(Motion agreed to)

The Chair: Thank you very much.

Our orders of the day, pursuant to the order of reference of Monday, April 28, are that we commence consideration 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 are fortunate to have here today the Honourable Peter Gordon MacKay, the Minister of Justice and Attorney General, with his staff to kick off the discussion of this legislation that has been referred to this committee.

Minister, the floor is yours.

Hon. Peter MacKay (Minister of Justice and Attorney General of Canada): Thank you, Mr. Chair, colleagues.

I am pleased to be joined by Justice Canada officials. We are here to answer questions with respect to Bill C-13.

[*Translation*]

I am very pleased to be before the committee to speak to Bill C-13, Protecting Canadians from Online Crime Act.

[*English*]

Chair, colleagues, I submit to you that Bill C-13 is an important piece of legislation aimed at protecting Canadians from crimes that are committed over the Internet or online. It does so in full compliance with Canadian law.

One of the ways in which Bill C-13 accomplishes this important goal is by proposing a new criminal offence aimed at a particularly contemptible and insidious form of cyberbullying involving the non-consensual distribution of intimate images. It has literally resulted in the devastation of lives, the loss of lives. I can't help but think of young Rehtaeh Parsons, Amanda Todd, Todd Loik, and others who have fall victim to this insidious type of activity.

The second way in which Bill C-13 accomplishes this goal of protecting the public is by proposing changes that would ensure that the Criminal Code and other federal legislation is able to keep up with the high speed of technological change. The need to modernize is deeply embedded in this overall intent.

In this vein, Bill C-13 proposes some minor updates to existing offences while at the same time modernizing the judicially authorized powers that police use, to investigate crimes committed, using electronic networks or that of electronic evidence. I stress for emphasis that “judicially authorized” authority is invoked here.

Turning first to the issue of cyberbullying, as I mentioned, the bill proposes a new Criminal Code offence prohibiting the non-consensual distribution of intimate images. Essentially this offence would prohibit the sharing of sexual or nude images, as defined, without the consent of the person depicted. It is a very nasty, cruel attempt to humiliate or worse, and has, as I mentioned, a pernicious effect that has become all too prevalent, particularly amongst young people.

This proposed new offence would fill a gap in the criminal law, and respond directly to one of the recommendations made by federal, provincial, and territorial officials in the June 2013 report on cyberbullying and non-consensual distribution of intimate images.

It may be of interest to note, Chair, that this report received unanimous support from federal, provincial, and territorial ministers of justice and public safety. These sections around intimidation, harassment, and related sections in the current Criminal Code context go back to age of the rotary dial telephone, so the need for modernization is real.

The proposed bill has a three-part definition of intimate images. In short, an intimate image is one that depicts nudity or sexual activity, was taken in a private setting, and one in which the depicted person has a privacy interest. This approach, like the existing voyeurism offence in section 162, is similarly designed to protect the privacy of the person depicted.

Clearly this Criminal Code section and the accompanying sections are not the entire answer. It will require a much more holistic strategy, as members of this committee are aware. There is much public information-sharing and education involved. We need to reach out to the schools. We need to have law enforcement and the justice system itself more broadly involved. There have been numerous public information efforts undertaken, including pink days and anti-bullying days that are dedicated at various sports and entertainment venues. It will require that holistic approach.

[*Translation*]

The bill also includes a number of complementary amendments related to the proposed new offence.

For example, the court would be authorized to order a person in possession of intimate images to enter into a recognizance to keep the peace, when there are reasonable grounds to believe that the person would commit the proposed new offence.

● (1145)

[*English*]

In addition to pre-emptive action, such as peace bonds, which have that ability to deter, the court would also be authorized to order the removal of non-consensual posted intimate images from the Internet.

Further, Mr. Chair, upon conviction under this new offence section, the court could order a seizure of equipment—a computer or a hand-held device—make a prohibition order restricting the offender's access to the Internet or other digital networks, and order the offender to pay restitution to permit the victim to recoup expenses incurred by securing the removal from the Internet of non-consensual posted intimate images.

This bill also proposes to modernize investigative powers. These updated tools would assist police in the investigation of not only the proposed new offence, but also all online crimes and any crimes that involve digital evidence, such as, for example, fraud or the distribution of child pornography. These amendments are long overdue, I suggest, and police report that over 80% of major crimes now leave electronic evidence.

While Canadian law enforcement continues to use investigative tools that pre-date the Internet and were primarily designed to collect physical evidence, there's great work being done, as I'm sure the committee is aware, at the Canadian Centre for Child Protection. They do tremendous work and outreach with police forces across this country and with victims.

I would like to be clear that while some of these amendments were previously introduced in a former bill, Bill C-13 does not contain the most controversial aspects of warrantless access. Mr. Chair, in particular Bill C-13 does not include any provision that would allow the warrantless access to subscriber information or that would impose obligations related to telecommunication infrastructure modification.

These amendments relate to investigative powers and were strongly recommended by the same FPT working group that recommended the new proposed offence to respond to cyberbullying and the non-consensual distribution of intimate images. This working group recognized that the important link exists between the proposed new offence that affords the protection and ensuring that police have the necessary tools with which to investigate it and other related online criminal activities. It is, I would suggest to you, very much intertwined—the new offence and the ability to police and enforce under the current provisions.

To give you a quick example of why these modernizing amendments are needed, we need to look at basic but essential telecommunications data, a phone number and an IP address. To obtain a phone number, police can then use the existing built-in production orders in the number recorder warrant, proposed subsection 492.2(2). This is granted by a court on reasonable grounds to suspect. That is the standard. To get the same type of information in an Internet context, such as an IP address or an e-mail, police currently have to use a general production order, which is granted on reasonable grounds to believe, which is a different, higher standard.

This is not only an inconsistent treatment of similar types of information, basic information, it also means that in many cases police, in the context of an Internet crime, will not be able to meet the threshold to begin an investigation. Bill C-13 proposes to correct this.

In terms of reasonable grounds to suspect, I want, Mr. Chair, if I could, to take you through a few of these modernization proposals. One of these proposed new tools is data preservation. Essentially, the data preservation tools are known as “not delete” orders, which would allow police to ensure specific computer data is safeguarded while they apply to the court for proper authorization to acquire that data in order to preserve important evidence. We have police officers, I know, who are part of this committee and can speak to that important preservation exercise.

These tools will provide essential support in the investigation of offences where much of the evidence is in electronic form. It is an era where crucial evidence can be deleted—sometimes inadvertently, sometimes deliberately—with a keystroke. Police, I suggest strongly, need this power.

The data preservation scheme includes a number of important safeguards. For example, once a preservation demand or order has expired, the individual in question is required to delete all the information he or she preserved unless retaining it is part of his or her normal business practice.

Bill C-13 also proposes to update the existing judicially supervised production order scheme. These amendments would result in a comprehensive tool kit that would include a general production order, which is comparable to a search warrant, and four specific and more narrowly focused production orders that will often help police initiate their investigations.

● (1150)

The four specific production orders contemplated by Bill C-13 would allow police to obtain four types of information: first, data to determine whether someone or something was at a specific moment in time, so it's tracking data; second, data that relates to the occurrence of telecommunications, such as an email associated with the telecommunications, so it's transmission data; third, data to trace a telecommunications item in order to determine the identity of a suspect; and finally, basic financial information such as a bank account number or the mere existence of an account of a particular person. It should be noted that this production order for financial information is already in existence.

The bill also proposes to modernize two existing judicial powers, warrant powers: the tracking warrant and the number-recorded warrant. These warrants are unique in that they allow police to collect the type of information in real time, and although the bill has been criticized in the media in particular for lowering judicial scrutiny, I would submit and point out that the proposed tracking-warrants amendments that apply to the tracking of individuals actually raise the standard of judicial consideration from "reasonable grounds to suspect" to "reasonable grounds to believe". This increased privacy protection recognizes advancements in technology and their impacts upon individual privacy. However, police continue to be able to track things under the existing "reasonable suspicion" standard.

Finally, the bill also proposes amendments to achieve some efficiencies with regard to wiretap applications. These amendments will ensure that Canadian courts in all jurisdictions will use the same processes when they seek to obtain court orders related to wiretap authorization. The proposed amendments would create a single application for judicial warrants and orders that are related to the execution of wiretap authorization. This new process would clarify that the judge who issues a wiretap authorization can also issue the other supporting warrants or orders without requiring a separate application. In some jurisdictions, police have to go before several judges for these related powers, such as tracking warrants, a process that not only is inefficient but that also prevents the judge from getting the full picture of the investigation.

Lastly, Mr. Chair, I would like to take just a moment to address a few of the misconceptions that have been reported on Bill C-13.

Some have mistakenly led others to believe that the proposed legislation would encourage telecommunications service providers and banks to disclose information on their customers without authorization. I want to be very clear. The proposed legislation would not provide the police with any new powers for voluntary disclosure, nor does the bill propose to create a mechanism to bypass the necessary court oversight. To start the provision in question, proposed section 487.0195 is a "for greater certainty" provision and as such cannot grant police any additional powers. These provisions exist to clarify what is already part of the law. As part of their general policing duties, police may already obtain information from a third party voluntarily, without a court order, if—and this is the important part—the person or organization is not otherwise prohibited by law from providing this information. For example, they can already assist police in providing information if they are not prohibited by their duties under the Personal Information Protection and Electronic Documents Act, the PIPEDA. Persons who assist police in that fashion are protected from liability in those cases.

To be clear, this power exists in common law already. The 2004 clarifying amendment was meant to preserve this common-law power. It is found re-enacted here in this bill, and is intended to do the same. The proposed amendments in Bill C-13 are not designed to alter this in any way but are meant to make the provisions clearer and more transparent.

It was also suggested that the bill creates new warrants for police to obtain metadata using a lower threshold production order. This is also incorrect. Metadata refers, as members would know, to a large class of information that has been described as data about data. Examples of metadata include background information about an electronic document such as software, the type that it uses, its size, kilobytes, the size of characters it contains, etc. In relation to an electronic photo, it can include the number of pixels, the type of camera, and perhaps the date, the time, and the location the photo was taken. Some have suggested that metadata may contain personal information about people. It should be noted that Bill C-13 does not propose to capture this type of information according to its proposed definition of transmission data.

● (1155)

In fact, the definition of transmission is narrowly defined and captures only data that relates to the act of telecommunication. The definition of transmission data is the modern equivalent of phone-call information, not what is actually contained in the conversation, and these proposals are meant to ensure consistent treatment of similar information.

To conclude, Mr. Chair, I want to emphasize that this package of reforms is a targeted approach to serious forms of cyberbullying. All of the amendments to the investigative powers have been proposed here to provide police the appropriate tools to investigate crime in this Internet age, while at the same time minimizing the privacy impacts on Canadians.

I thank you for your consideration, and I look forward to your questions.

The Chair: Merci.

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

[*Translation*]

Ms. Françoise Boivin (Gatineau, NDP): Thank you, Mr. Chair.

Mr. Minister, thank you for being here. Once again, this meeting has been shortened because of a time allocation motion by your government on another bill.

Having said that, I appreciate the fact that you seem to want to fix some of the bad impressions that Bill C-13 left with experts in the protection of privacy and other areas. However, the fact that all those voices were raised against the bill the same day it was tabled and that those people saw some concerning similarities between it and Bill C-30 suggests to me that, in practice, after the Conservatives have passed it in the House, Bill C-13 may not be as clear as you seem to believe. That concerns me a little and I end up asking the same question every time you come and present us with a new government bill.

The short title you have given to Bill C-13 is the Protecting Canadians from Online Crime Act. However, it touches on much more than online crime. In fact, it also includes a very limited section on distributing intimate images.

After drafting this bill, did you have it checked? I know you have your officials from the Department of Justice, but did you consult with your experts on the Constitution and the Charter to determine whether the bill would pass the tests we all know it will inevitably be subject to? It seems to be the fashion for the Conservatives to find themselves before the Supreme Court. Do you have assurances aside from just your personal perception that everything is hunky dory? Have you received serious legal opinions that give reasonable assurances that your bill will hold water in a very high percentage of cases, and not just in 5%, 10% or 15% of cases?

Hon. Peter MacKay: Thank you, Ms. Boivin. It is always a pleasure to answer your questions. I know you are quite interested in this area.

Of course, for this bill as for all the others, it is necessary to seek the opinions of Department of Justice officials in order to determine its constitutionality. We make sure to do it in the case of an initiative or a bill that affects the privacy rights of Canadians.

[*English*]

You mentioned the fact that we seem to be pre-emptively discussing some of the mythology around this bill. Clearly, this legislation had a predecessor bill that I think raised alarms, and that's why I highlighted the particular issue around warrantless access. This bill does not contain aspects of warrantless access. This bill goes right to the very heart of the necessity to have judicial oversight.

Similarly, I highlight again the fact that the provinces and territories were quite adamant about the necessity to move in this direction, and that report was very instructive in the drafting of this legislation.

Ms. Françoise Boivin: Are you talking about the report on

[*Translation*]

…cyberbullying and the non-consensual distribution of intimate images?

Hon. Peter MacKay: Yes, exactly.

Ms. Françoise Boivin: Yet everyone agrees that this barely affects sections 2 to 7 and section 27. For everything else, I don't think this report is specific enough to justify the 40-odd other sections that make up the bill.

● (1200)

[*English*]

Hon. Peter MacKay: With respect, Madam Boivin, it would be, I suggest, a hollow effort to bring forward legislation that was aimed to protect people from online or cyber abuse and not have the ability to police or to enforce those particular—

Ms. Françoise Boivin: I disagree with you on that one, Minister. Honestly, I agree there need to be tools, but what I submit to you is that you might not have reviewed the aspect of the tool as much, especially in view of the backlash your government received against Bill C-30. As for cyber-intimidation, it is pretty much unanimous—everybody agrees there's a need to do something about it.

I go back to the core of my question. What type of review have you done to make sure that when you introduce a new concept—because I agree they do need a warrant, but you have changed the burden of proof....

[*Translation*]

It is no longer the same thing. Every lawyer who practices criminal law is familiar with the principle of having "reasonable grounds to believe". You are also familiar with it because you were a Crown prosecutor and a defence lawyer. Yet suddenly we are talking about "reasonable grounds to suspect". New concepts are being introduced here.

Did you have these concepts tested before introducing Bill C-13, which will have a lot of ramifications beyond cyberbullying and the distribution of images? In fact, this bill casts a very wide net.

[*English*]

Hon. Peter MacKay: Madam Boivin, I know and I greatly respect the fact that you, as a practitioner, follow these issues so closely. You would know that this concept of reasonable grounds to suspect is now in place. It has been accepted by the courts. It has been tested. It's constitutionality has been accepted, and for low-level privacy matters, I would suggest it has become the standard. We are simply codifying that with respect to the police investigative powers for certain types of privacy infringements, if you will.

As you know, you are always balancing the ability to protect the public, and I would suggest that this issue and the insidious nature of cybercrime demands that we give police the power to at least meet that threshold of starting an investigation. As they attempt to get more private information that would be considered of a more intrusive nature, they have to equally, and with a commensurate level of oversight, hit a higher threshold of reasonable grounds to believe. Just as we move our way through the courts and then get to that much higher standard of proof beyond a reasonable doubt. It is part of that continuum as you can appreciate that gets police in the door if you will, or online.

Ms. Françoise Boivin: So “suspect” is lower than the other.

Hon. Peter MacKay: “Suspect” is a lower threshold, but it has been accepted and, I would suggest, tested by the courts.

The Chair: Thank you for those questions. Thanks for those answers.

Our next questioner is from the Conservative Party, Mr. Dechert.

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

Thank you, Minister, and to your officials for joining us today to talk about this important bill.

Minister, last week when I was in my constituency, I listened to a speech by Chief Jennifer Evans of the Peel Regional Police. She mentioned in her speech that her police service had done a survey of the concerns that people have in Peel Region, some 1.4 million people, on criminal justice issues. She said that the number one issue for people in the Peel Region is school safety and bullying. Every parent across Canada is concerned about the issue of cyberbullying and intimidation over the Internet.

I know that our government believes in an equilibrium between prevention and prosecution. We believe that victims deserve justice and that authorities at every level must participate to prevent crimes on the Internet.

Could you tell us about some of the initiatives put forward by our government to prevent crimes on the Internet?

Hon. Peter MacKay: Thank you, Mr. Dechert.

I think your community, the Peel region, which I've had the pleasure to visit on a number of occasions, and where I've participated with you in public events and round tables, is reflective of a view held in many communities.

We've heard of the high-profile tragedies of cyberbullying and the resulting terrible ripple effect it has had. Yet, at the same time we've identified gaps in the criminal law, which this particular legislation means to fill. Similarly, the accompanying effort to empower the police to be able to enforce and essentially to have the effect that is desired.... By creating a new criminal offence around the distribution of intimate images, as well as this enabling legislation, this bill is meant to respond to these needs, and to do so, as you suggested, in a preemptive way akin to a peace bond. It does because when we see escalated behaviour online and the ongoing pernicious effect of bullying, which used to be confined to a schoolyard or to a playground, it now literally follows a young person home, into the classroom, and into every walk of their life, and has such a humiliating and devastating effect on them. We know that young people are in some ways more susceptible to this because of social pressures. This is a pressing concern that we are attempting to address here.

We've consulted broadly on this. I talked about federal-provincial-territorial consultation, but we've heard from many groups. I suspect you will hear from very informed and, in some cases, very emotional people who will come here and testify about how this has affected them and their families. So we're doing this in a way that we hope conforms with the intent of other bills, including the victims bill of rights, which you and members of this committee, we hope, will have a chance to examine in the near future. We're doing this consistent with other legislation aimed specifically at protecting children from sexual abuse, including luring and the very dangerous type of entrapment that often occurs online.

So there is a consistency and a theme here of protection and prevention that runs through this bill and other legislation I've referenced.

Thank you for that question.

● (1205)

Mr. Bob Dechert: Thank you, Minister.

As you know, Mr. Allan Hubley is a City of Ottawa councillor and a father of a bullied teen who took his own life rather tragically. Last November, when this bill was introduced, he said, “When we were younger, you always knew who your bully was, you could do something about it. Now, up until the time this legislation gets enacted, they can hide behind that”—the Internet, that is. He said that on *Canada AM*. He went on to say, “Not only does it start to take the mask off them, through this legislation there is serious consequences for their actions.”

Can you explain to us why it is so important to modernize the current Criminal Code?

Hon. Peter MacKay: Thank you for that question, Chair.

Mr. Chair, I fear there has been an evolution around this type of online behaviour that we all know is very cowardly. That stems from the anonymity of the activity that takes place online. Criminals can take advantage of the mask that exists on the Internet. The investigative powers of the Criminal Code need to be modernized to address that fact and to facilitate the investigation of criminal activity that involves this type of electronic communication.

This is, to coin a phrase, the modern *Lord of the Flies*, where there can be a group mentality that results in the type of sustained bullying of an individual, young or old, that can have an absolutely life-altering and sometimes life-ending effect. Allan Hubley's comments are not only relevant but also very poignant, given the situation that he and his family found themselves in.

The Criminal Code already has a variety of tools for accessing information. This bill allows for production orders, interceptions, authorizations, and search warrants. But most of the tools that are in the code now were put in place in the 1990s. That's the last time we had a modernization. That was before cell phones, the Internet, and hand-held devices were so common. The explosion of online activity is well known to all.

Not only are we falling back but we are out of step with other modern countries that have already moved in this direction. So I would suggest there is urgency, as I mentioned. Even the latest additions we've made around production orders and certain tools that are to be made available to police, go back almost 10 years, to 2004.

Existing tools, I suggest, are inadequate. They weren't put in place with this type of electronic world in which we now live in mind, where digital evidence is often volatile and crucial to pursue and prosecute cases, and to respond at the speed of light. When somebody presses a button on a device, it can literally go around the world quickly. So these practical amendments and this forward-looking legislation, I suggest, are absolutely crucial in our effort to keep people safe.

● (1210)

The Chair: The next questioner from the Liberal Party is Mr. Casey.

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

Mr. Minister, I want to focus in on a proposed section that you referenced in your opening remarks. You know I've been a bit preoccupied with this proposed section 487.0195. If I understand what you said in your opening statement, it was that law enforcement presently has the power to obtain, without a warrant, information from telephone companies on a voluntary basis. They presently have that power. This statute recognizes that they have that power. Have I fairly characterized what you said?

Hon. Peter MacKay: Yes, that's correct. They currently have the power under the Criminal Code, as well—under the broader section 25 of the Criminal Code, which empowers it.

Mr. Sean Casey: I think what you also said is that, when they exercise that power, the telephone companies that are voluntarily cooperating with police and providing information without a warrant have a common law immunity from class action lawsuits and criminal prosecution. They have a common law immunity that this statute has codified. Do I understand you correctly on that point?

Hon. Peter MacKay: It would have been codified in 2004, in fact, Mr. Casey. That was the latest update to the section we're referring to here, proposed subsection 487.014(1).

Mr. Sean Casey: So, what would proposed subsection 487.0195 (2) do, if that's the case?

Hon. Peter MacKay: Well, it is basically a re-enactment of the existing section, which has been renumbered primarily to accommodate the new preservation of production orders that are found in this bill. Its purpose is also to spell out, more clearly than in the previous version, that a person assisting police would be able to benefit from the protection that's offered by the Criminal Code. So, for those who voluntarily provide this type of information to assist law enforcement—if it's reasonable in the circumstances, if it's in compliance with the law, which it must be, including contract law and law that is governed by the protection of information that was provided—this is a re-enactment of that existing section. So, it is there for emphasis. I think, in simple parlance, because of the technical complexity of this bill and the very legitimate concerns that people have about the protection of their privacy, it bears that emphasis.

Mr. Sean Casey: So, Minister, would you agree that Bill C-13 codifies an immunity for telephone companies from class action lawsuits when they cooperate with warrantless, but lawful, demands for documents?

Hon. Peter MacKay: If it is deemed lawful, then they should be immune from prosecution. But, to be clear, Mr. Casey, this bill would not create any new protection from any criminal or civil liability for anyone who would voluntarily assist law enforcement. It simply clarifies existing provisions and protections.

Mr. Sean Casey: In the circumstances that I just described, the circumstances where you have a warrantless but lawful request made by law enforcement to a telephone company, do you agree that in those circumstances the telephone companies have no obligation to disclose to their subscribers that they have given this information to authorities without a warrant, albeit lawfully?

Hon. Peter MacKay: That really is an issue that is covered under the PIPEDA. It is really, as well, potentially an issue of contract law between the individual and the service provider, the company. But the provision provides protection for those who are voluntarily assisting police in an investigation, where such assistance is not otherwise prohibited by law. So, the element of protection, if you will, or immunity has to respect the common law provision of voluntary disclosure as well as any existing contractual obligations that may exist. It must be done in a way that complies with section 25 and this other section that you're referring to, 487.

● (1215)

Mr. Sean Casey: While we're on the subject of PIPEDA, you're undoubtedly aware, Mr. Minister, that presently before the Senate is BIll S-4, which proposes some changes to PIPEDA and will actually relate to the section that we are presently discussing.

Hon. Peter MacKay: Bill S-4 amends PIPEDA. It's currently before the Senate and—

Mr. Sean Casey: Let me finish my question, if you would, please.

One of the things that Bill S-4 would do is to expand the parties to whom telcos can, on a secret and warrantless basis, provide information. Right now, the only people that telcos can provide this information to are law enforcement authorities. This will broaden it, is that right?

Hon. Peter MacKay: I would not necessarily agree with that. Persons who disclose personal information without a warrant must do so in accordance with PIPEDA, and the Criminal Code does not compel unwarranted disclosure of personal information. What paragraph 7.(3)(c.1) of PIPEDA talks about is an order by a government institution or part of a government institution that has made a request for the information, and has “identified its lawful authority to obtain the information”.... There are repeated references to the necessity for lawful authority.

Mr. Sean Casey: I don't dispute that—

The Chair: Very quickly.

Mr. Sean Casey: —but perhaps I haven't framed....

Here's what I'm putting to you, Mr. Minister. Right now, the only people who can avail themselves of the warrantless powers of voluntary disclosure are those in law enforcement agencies. Bill S-4 would allow anyone who's investigating any breach of contract from any organization, whether private, public, government or not, to avail themselves of that power.

Hon. Peter MacKay: I come back to the fact that it has to be done in compliance with the criminal law, it has to be done in accordance with PIPEDA.

Mr. Sean Casey: We agree on that.

Hon. Peter MacKay: I'm not here to discuss Bill S-4. Even if I were, we don't have that legislation in front of us here. So I'm not going to get into the provisions of a bill that we're not here to discuss.

Mr. Sean Casey: They fit together.

The Chair: Thank you, Mr. Casey, for those questions. Thank you, Minister, for those answers.

Our next questioner is from the Conservative Party, Monsieur Goguen.

Mr. Robert Goguen (Moncton—Riverview—Dieppe, CPC): Thank you, Mr. Chair.

Thank you, Minister, and the officials for coming to testify today.

I think most Canadians share with you the urgency of putting in place this important piece of legislation. I think of victims like Rehtaeh Parsons, from your home province of Nova Scotia. Her family and many other Canadian families would certainly agree that something has to be done about a faceless bully on the Internet.

In the context of cybercrime, of course, the preservation of evidence is always first and foremost. Without it there can be no prosecution and no conviction of those who are perpetrating the harm. We know that the working group on cyberbullying strongly recommended that the federal government enact investigative tools and procedures enabling law enforcement to keep pace with modern technology.

We've talked about some authority and some provisions that were already in place, but there are obviously new provisions. Could you highlight for us what the new data preservation scheme would be, Minister?

Thank you.

Hon. Peter MacKay: Thank you very much, Mr. Goguen. Thank you for your work and your interest in this.

I would suggest that given the insidious nature of some of the online activity that we're talking about here, as in all things in the criminal law it requires balance. Bill C-13, I would suggest, very much seeks to strike that balance, and you will have to a chance able to hear from others on this as well. It creates a new data preservation scheme. The tools are intended to allow police to safeguard and preserve necessary evidence. Mr. Wilks, as a police officer, can certainly speak to the importance of the police ability to do just that.

This is about the preservation of a virtual crime scene that we're talking about. It also seeks to prevent deliberate or accidental interference in the administration of justice by having that critical data, that critical evidence, disappear. While this bill doesn't create additional obligations for telecommunications companies, it does very much put in place a practice in which police can preserve that important information, that data and evidence. It does not require them to retain data or develop new infrastructure, but it requires that do-not-delete orders to be respected, which I would suggest is critical, to answer your question.

Another feature of this bill in seeking balance around privacy and investigation is that once the demand or order requiring the preservation of that evidence has expired, that is, the order not to delete certain computer evidence, the Internet service provider is free, of course, to act however they choose, whether they normally preserve all the data or choose to delete it, as you would expect in the physical world. Once an investigation has been completed or a warrant has expired, there is no further legal obligation.

So it is in keeping with existing police and court practices around warrants and around seizures, while at the same time responding to the very real technical aspect of how data is preserved, relayed, and treated in the Internet and the electronic world.

● (1220)

Mr. Robert Goguen: Thank you, Minister.

To take up on something Madam Boivin was saying, by and large the most essential parts of this bill have been well accepted by Canadians. It's pretty obvious that putting nude photos on the Internet and distributing them without somebody's consent is certainly something that's wrong and should be curtailed.

Some of the provisions that have attracted some media attention relate, for instance, to cable theft, which quite frankly I thought would have been covered already in the Criminal Code. Could you comment exactly why this has been added into this bill, cable theft being an example that comes to mind?

Hon. Peter MacKay: Thank you, Mr. Goguen.

Again, your legal background is shining through. You would know that it's already illegal to steal cable. It has been part of the Criminal Code since 1975. So this is not new. To steal cable, to steal signals, to possess a device used for telecommunication theft, this has been something that has been codified for many years. The behaviour is prohibited in other sections 326 and 327. It's a type of theft.

What we're again attempting to do is modernize through this Bill C-13 and these longstanding offences and the update around telecommunication language to expand the conduct that it covers and to make it consistent with other offences is what is found in this bill.

It would add, for example, imports or makes available. That type of language gets to the subject of transmitting inappropriate images, the type of images, nude images that can be most offensive and most humiliating for individuals. The approach itself, in principle, I would suggest, is not a substantial change. It is consistent with previous practices and code sections.

Moving onto the police investigation part, the tools that enable police to do their work to investigate, it includes updates to the existing Criminal Code production order provisions that deal with things such as financial data and transitions, because we know that Internet white-collar-type crime, fraud, is also very pervasive. This bill empowers police in that regard to preserve and get at necessary data, financial data in many cases, to help them build a case that protects citizens, to protect individuals who may fall victim to those predators who use the Internet to perpetrate financial fraud and crime. It's part of other efforts that are made by financial institutions themselves, the other legislation around proceeds of crime, money laundering, terrorist financing. These are all issues that are intertwined and, I would suggest, that are consistent with the effort found in Bill C-13.

The Chair: Thank you for those answers, Minister.

Our next questioners are from the New Democratic Party.

Mr. Jacob, I'll let you know when you've used up three minutes because I understand you'd like to share your time.

● (1225)

[*Translation*]

Mr. Pierre Jacob (Brome—Missisquoi, NDP): Thank you, Mr. Chair.

Mr. Minister, thank you for being here this afternoon.

I would like to share my time with Ms. Boivin, as the chair indicated.

My first question has to do with clause 27 of the bill, which deviates from traditional common law and sets out that the prosecution may compel the spouse of the person accused of distributing intimate images to testify.

Is that provision still necessary? Is it redundant, given that Bill C-32, Victims Bill of Rights Act states that the prosecution may compel the spouse of the accused to testify in the case of any offence?

Hon. Peter MacKay: That is a good question. I would like to clarify that Bill C-32 on the Victims Bill of Rights has not yet been passed; it is currently being studied by the committee. I introduced this bill so that we can ensure that all the evidence is before the court in the case of prosecutions.

Mr. Pierre Jacob: Could the prosecution also force the spouse to disclose communications made during the marriage?

[*English*]

Hon. Peter MacKay: I think your question about private communications is not covered or contemplated. We're talking about evidence that they would offer specific to the criminal offence that would be of value and relevance to the charge, whatever that charge might be. So private communications between spouses I don't believe are compellable under this particular section.

[*Translation*]

Mr. Pierre Jacob: I have time for one more question.

Canada signed the Council of Europe's Convention on Cybercrime in November 2001, as well as its additional protocol on hate crime in July 2005, but has not yet ratified them.

Will Bill C-13 be used to ratify the Convention on Cybercrime?

[*English*]

Hon. Peter MacKay: The short answer is yes, *mais oui*. I would note as well that we are the last of the G-7 countries not to have done so, and so I would consider this part of the enabling effort and encouragement for Canada to do so. We want to be on a par or at least equal to those countries. It's not enough to just sign. This demonstrates real action.

[*Translation*]

Mr. Pierre Jacob: I will turn things over to Ms. Boivin.

Ms. Françoise Boivin: Thank you, Pierre.

Mr. Minister, I have just enough time to ask you a quick question.

In his Bill C-279, my colleague Randall Garrison adds the expression "gender identity" to section 318 of the Criminal Code. Do you have an objection to amending clause 12 of Bill C-13 in a similar way to include gender identity in the definition? It would be good to know that ahead of time, because it could provide an indication to the Conservative members of the committee.

[*English*]

Hon. Peter MacKay: In principle, I don't have difficulty with this. You're referring, I believe, and please correct me, to all forms of hate propaganda—

Ms. Françoise Boivin: Yes.

Hon. Peter MacKay: —and anything that would perpetrate identifiable persons as a cause for hate or inciting violence, so in principle—

Ms. Françoise Boivin: Then it would be in compliance with what has been adopted by the House of Commons anyway, Bill C-279, which is sleeping in the Senate right now like a lot of other bills.

Hon. Peter MacKay: That is correct, so hopefully this might awaken them from their slumber.

● (1230)

Ms. Françoise Boivin: Thank you, Minister.

The Chair: Thank you very much.

Minister, I want to thank you very much for taking the balance of the full hour with us.

Our last questioner from the Conservative Party is Mr. Wilks.

Mr. David Wilks (Kootenay—Columbia, CPC): Thank you very much, Mr. Chair, and thank you, Minister, for being here.

I want to go back if I may, Minister, to what Mr. Casey was speaking to because I must say I get a little perplexed when I hear the word "warrantless" and "police" in the same sentence because it's just not true.

Is there volunteer information provided that police ask for, and if it subscribes within the law; yes, that's exactly what's happened. It's volunteered.

The other thing I want to say, Minister, was as an author to a Part VI investigation, I completely agree with you that oversight is ramped up significantly as the investigation goes on, right to a Supreme Court justice.

One of the things I wanted to ask about was about proposed section 487.0194, which falls into proposed subsections 487.0195(1) and (2), and that is with regard to the preservation demand, form 5.001; the information to obtain a preservation order, 5.002; followed by the preservation order itself, 5.003.

Could you tell the committee how those correlate to 487.0194 and what they are meant to do for the police because we used to use a preservation order, all the time, prior to getting the warrant.

Hon. Peter MacKay: In that 30-second question you have really demonstrated, for all present and all tuning in, the complexity of this and the onerous requirements on police to not only understand the law but also to carry out their duties in a way that complies with not only the Criminal Code but other legislation including PIPEDA. I'll try to answer your question, and if I might say so it's great to have a practitioner here who will be taking part in this important examination of the bill. I commend you for that, Mr. Wilks.

What is a preservation demand? As you know, this is a legally binding request from law enforcement to be able to go out and seek to gather evidence, to seek to have that evidence prevented from disappearing, in the virtual context of the Internet we're talking about here. The new aspect of this, where you can ask at a minimum standard that evidence not be deleted, is what we're attempting to put in place here. To give the police the ability to say that until we're able to gather this evidence, you, the holder of this evidence, cannot make it disappear. Whether intentionally or otherwise, you cannot prevent us from taking a look at that important evidence that we feel will further our investigation. It may exonerate, which is another very real possibility in the examination of evidence.

What we're attempting to do here doesn't give authority to access the actual information. It simply says that we want you to preserve it, to hold onto it until such time, in most instances you can get that higher threshold of judicial oversight, that says now you can go in and look at the actual content of what may be there.

In old-fashioned terms, it's to prevent somebody from interfering with a crime scene. I believe it's meant to ensure that the data will exist when the police come back with the proper judicial authority to go further. It's non-renewable, so it puts a limit on the time in which police have to act, which is fair, and if authorities don't return within a certain amount of time, then the owner, the possessor of that material, has the right to do with it what they please. In fact, very often it may be erased or deleted.

Disclosure of historical information, court order, third-party involvement—all of this is covered, and it is on that standard of "reasonable grounds to believe", which you are very familiar with.

Thank you.

The Chair: Thanks for those questions, Mr. Wilks.

Thank you, Minister, and thank you for spending the time.

The officials are going to stay until 1 o'clock for us. I don't know if they knew that or not, but there are some questions for officials only.

I'm going to suspend for about 30 seconds so the Minister can leave.

Thank you very much for your participation today.

● (1230)

(Pause)

● (1235)

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

First of all, let me start with an apology. I always make the mistake of calling officials "staff". I spent 13 years in municipal politics, and we called our officials staff. I'm still not used to calling the bureaucratic level "officials" here; I still call them staff so I apologize for that. I know I went right in to the minister so I didn't get a chance to introduce you before because I wanted to save time.

Mr. Piragoff is here. He is the senior assistant deputy minister in the Department of Justice. Mr. Wong is also here from the criminal law policy section, as is Madame Audcent, who is a senior counsel. We have some questions for you, and we're going to start with Madame Boivin from the New Democratic Party.

[*Translation*]

Ms. Françoise Boivin: Thank you, Mr. Chair.

I like the fact that we can use the term "maître" in French to designate these individuals. Actually, I think it is used almost exclusively here for lawyer.

Thank you for being here, despite your busy schedule. The Standing Committee on Justice and Human Rights keeps you very busy, no doubt.

My questions concern the offence of distributing intimate images. In preparation for these hearings, I met with a lot of groups, obviously, and they shared their concerns with me. That is the case for representatives of Facebook, something we are all familiar with. We will very likely hear from them during the committee's work. The offence as worded in Bill C-13 could be perceived as much broader than intended. In short, there are certain concerns, and I will share them with you.

Among others, under the provisions on the offence of distributing intimate images, which is the new section 162.1 proposed to be added to the Criminal Code, the accused cannot be deemed guilty if the person in the image gave his or her consent. Therefore, if a minor consented to the distribution of the image, it is likely that the author will not be charged under the new section 162.1, which allows consent as defence, but instead under the offence of child pornography, which does not allow that defence. However, the sentences are much harsher for child pornography. If the accused obtained the minor's consent, could the accused be charged with child pornography and receive a harsher sentence than if the accused had not obtained the minor's consent, in which case the accused would be convicted of distributing intimate images?

We are also talking about not attempting to obtain consent; in other words, letting things slide. As we know, things move so quickly, without necessarily being motivated by criminal intent. Some people are concerned that people are considered as having committed criminal offences and prosecuted as a result when they had absolutely no criminal intent.

What do you say to those people?

[*English*]

Mr. Normand Wong (Counsel, Criminal Law Policy Section, Department of Justice): Thanks for the question, Madame Boivin.

First of all, the offence is constructed in a way that the offence happens if intimate image is distributed without the consent of a person, or if the distributor is reckless as to whether or not that person consented to the distribution of that image.

Ms. Françoise Boivin: What does reckless mean exactly?

Mr. Normand Wong: Reckless is not inadvertent; it's not by mistake or because you weren't paying attention. Recklessness is a subjective mental element in the criminal law, and it's where someone recognizes a substantial risk and proceeds anyway. For example, if someone finds a picture of their classmate online and they know this person to be a virtuous person and they've known them for many years and they know they probably would never have consented to the posting or distribution of this image, but they decided to re-post it anyway or to sent it to friends, that's recklessness, where there's a substantial risk of knowledge, but the person decides to proceed anyway.

● (1240)

Ms. Françoise Boivin: What about the provider? Let's say Facebook. Can they or any other type of server be pursued in some aspect for the fact that they host the image? There are a lot of the questions right now on C-13.

Mr. Normand Wong: Again, this offence was constructed or modelled very much in the manner of the voyeurism offence. When you think of a voyeuristic picture, it could just be a nude picture of a person. On its face, it's not illegal. Unless intimate images are child pornography, on their face they are just legal pornography. If a service provider like Facebook or Google or whoever was dealing with this one, an ISP in Canada—Bell Canada or Rogers—found a picture like this, they would have no way of knowing it's an intimate image. There is a mechanism in the law that allows a person to make an application to a court for a judge to determine that it's an intimate image, and that judge can order that the image taken down if the image resides on servers in Canada.

Ms. Françoise Boivin: Am I wrong to say then that

[*Translation*]

...the scope of Bill C-13, with respect to the offence of distributing intimate images, is still fairly limited?

[*English*]

Mr. Normand Wong: It is limited. It's limited not only in relation to the definition of what constitutes an intimate image; it's limited in terms of the scope of who it might capture, too. It's not intended to capture the service providers who provide our telecommunications services.

Ms. Françoise Boivin: So it's only a partial element. I know you're not responsible for the titles of bills, but when I read

[*Translation*]

..."Protecting Canadians from Online Crime Act"...

[*English*]

in virtue of that very limited scope of distribution of an intimate image.... I mean, it's protecting, but it's not really doing everything to protect Canadians from cyberbullying. It's a limited aspect of cyberbullying, if I'm correct.

Mr. Normand Wong: You are correct vis-à-vis the new offence, but you have to remember that Bill C-13 covers more than the new offence. It also modernizes the Criminal Code, other substantive offences vis-à-vis modern technology, and provides police with the investigative tools they need to investigate Internet crime and any other crime involving electronic crime.

Ms. Françoise Boivin: Thank you.

The Chair: Thanks for those questions, Madam Boivin. Thanks for those answers, Mr. Wong.

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

Mr. Patrick Brown (Barrie, CPC): Thank you, Mr. Chair.

I have a few questions. The first is in regard to restitution. I understand that the penalties outlined in Bill C-13 include restitution so that victims can recoup some of the expenses associated with having images removed from the Internet or social media sites. I wonder if you could expand upon that and what it means.

While you look into that, perhaps I could ask an additional question.

In June of 2013, the working group of the coordinating committee of senior officials on cybercrime published a report, "Cyberbullying and the Non-consensual Distribution of Intimate Images". Can you comment generally on that report, who was involved, and what its main recommendations were as they relate to the bill?

Mr. Normand Wong: I'm sorry, I missed your last question since I was looking for.... But I am ready for the first question.

● (1245)

The Chair: Well, let's answer the first one, and I'll allow him to ask you the second one.

Mr. Normand Wong: The provision on restitution in section 738 of the Criminal Code was amended. This provision will allow a person whose intimate image was posted on the Internet to apply to a court for the costs related to the removal of that image. If those costs aren't easily ascertainable, then the court can also order reasonable compensation for the removal of those intimate images.

The Chair: Your second question.

Mr. Patrick Brown: In June of 2013, the coordinating committee of senior officials cybercrime working group published a report, "Cyberbullying and the Non-consensual Distribution of Intimate Images". Can you comment generally on this report? Who was involved, and what its main recommendations were and how they relate to this bill?

Mr. Normand Wong: I was involved. I chaired that group. The working group was a subgroup of the cybercrime working group. It was basically an ad hoc group, containing not only members from the federal, provincial, territorial working group on cybercrime but also any other interested FPT working groups. It met a number of times over the course of the spring and early summer to develop this report. As the minister said, it came to be unanimously accepted by FPT ministers of justice and public safety.

The recommendations of that report are reflected in Bill C-13 and both parts of Bill C-13, including the new offence and the complementary amendments for that new offence, as well as the modernization of the Criminal Code and the introduction of modernized and improved police powers for this Internet age.

I'm not sure if I've answered your question.

Mr. Patrick Brown: Yes, you did.

You touched upon the modernization of the code. One comment that's generally used in the context of the bill is that there already are a lot of tools within the Criminal Code and that the police already have a number of tools of their own. Could you comment on how the modernization and updating of the code helps in relation to terrorism, money laundering, and cable theft?

Mr. Normand Wong: You're picking up on some of the things that were mentioned by the media. In relation to terrorism there are some amendments to make the existing provisions consistent with other existing provisions.

Currently, from the Criminal Code, you can get the wiretap authorizations for up to a year in relation to organized crime or terrorism offences. So that timeframe was added to the number recorder warrant, which is being converted into the transmission data recorder warrant and the tracking warrant to make those consistent. That was done primarily because the tracking warrant and number recorder warrant currently are usually always obtained at the same time a wiretap authorization is obtained. Making the timeframes consistent means that the police don't have to constantly go back to the court every 60 days to make it go in line with the wiretap authorization.

In relation to cable theft, as the minister has mentioned, the theft of cable or telecommunications has been an offence in the Criminal Code since the 1970s. The only thing that we changed here is modernizing it, tinkering with the language to make it consistent with other similar or related provisions so that the courts would be able to interpret the scope of those provisions similarly and how they apply to persons who may commit those offences.

Mr. Patrick Brown: Thank you.

The Chair: Thank you, Mr. Brown.

Thank you, Mr. Wong.

Our next questioner is from the Liberal Party, Mr. Casey.

Mr. Sean Casey: Thank you, Mr. Chair.

The minister seemed quite reticent to talk about the interplay between Bill C-13 and Bill S-4. Am I okay to ask about that? Are the witnesses comfortable talk about that?

Mr. Donald Piragoff (Senior Assistant Deputy Minister, Senior Assistant Deputy Minister's Office, Department of Justice): I can talk about Bill C-13. Bill S-4 is another bill, and it's not our bill. That's the bill for the Minister of Industry, I believe, so that's his responsibility. You'd have to ask other officials or other staff, Mr. Chairman, with respect to that bill.

In terms of the interplay, as the minister said, the Criminal Code provision enacted in 2004 was enacted for the purpose of clarifying that when Parliament enacted production orders in 2004, the enactment did not have a negative effect on the common law power of citizens to voluntarily provide information to the police, whether it be telcos or whether it be a person at the door. When the police come knocking at the door saying that there was a big ruckus across the street last night and asking if they saw anything, the person at the door has the choice of saying that they don't want to talk to them or saying, “Yes, I saw a lot and here's what I'm telling you.” That person would be protected. That's the common law power. It's in section 25 of the Criminal Code.

There was a concern about having a power to compel people to provide information: would this have a negative effect on the voluntary ability of people to provide information? So section 487.014 was created at the time, for greater certainty. As it says, “for greater certainty”, the fact that there is a production order does not affect the ability of people to voluntarily provide information, and that provision also said that people who provide voluntary information get the benefit of section 25 of the Criminal Code. Section 25 of the Criminal Code is the provision that says if you do something that you are authorized by law to do, you are protected from civil or criminal liability.

What the new amendment does is update the existing section 487 provision to do two things. One, because there are other types of tools that have been created by the bill, such as preservation orders, if a company voluntarily preserves data, this makes it clear that not only in providing the data but also in preserving the data voluntarily, one would be protected from civil or criminal liability.

The current situation right now with many of the telcos, for example—you wanted to know the relationship, Mr. Casey—is that there is no ability to compel a telco or an ISP to preserve information. The authorities have voluntary cooperation from some telcos and some ISPs, but not all. Nevertheless, we do have some who do voluntarily cooperate with the police and will voluntarily preserve data while waiting for the police to come back with a search warrant or a production order.

This would, then, extend the immunity provisions to also include those individuals who voluntarily preserve data, to ensure they are not liable civilly or criminally because they voluntarily cooperated with the police. That's the relationship between the two, Mr. Casey.

In terms of what the authority is, as to when telcos or other companies are authorized or compelled to provide information, one would have to look at PIPEDA, and again, that's not in my purview of expertise.

● (1250)

The Chair: You still have time if you want it, Mr. Casey.

Mr. Sean Casey: As part of these hearings, we're going to have a witness testify who I know you're familiar with. Dr. Michael Geist is the Canada research chair in Internet and e-commerce law. I'd like to get your reaction to this comment:

> ...organizations will be permitted to disclose personal information without consent (and without a court order) to any organization that is investigating a contractual breach or possible violation of any law. This applies [to] both past breaches or violations as well as potential future violations. Moreover, the disclosure occurs in secret without the knowledge of the affected person (who therefore cannot challenge the disclosure since they are not aware it is happening).

Your response, please.

Mr. Donald Piragoff: I believe Mr. Geist's comments are in relation to Bill S-4, and I cannot comment on Bill S-4. It's not my area of expertise nor the Department of Justice's expertise. That is a bill of the Minister of Industry.

The Chair: Thank you, Mr. Casey.

Thank you for those answers.

The last questioner, for a couple of minutes, is Mr. Dechert.

Mr. Bob Dechert: Thank you, Mr. Chair. I'll be quick.

Ladies and gentlemen, I wonder if you could tell us anything that you know about the investigation of the Amanda Todd case. I think we were all relieved to hear recently that someone's been charged, and I realize it's a matter before the courts, but my question is about the investigative powers.

I saw one report that suggested that information on the identity of the person who was intimidating Amanda Todd came through an American ISP provider, and then someone was identified in the Netherlands.

Can you tell us anything about the provisions in this bill that would enhance the police's ability to investigate that type of crime in the future? Obviously, we all wish this crime could have been prevented in the first place. Is there something that the Americans have that we don't have that this will fix? Can you comment on that?

Secondly, how will the provisions of this bill allow authorities to prevent in future the kind of intimidation that Amanda Todd suffered?

● (1255)

Mr. Donald Piragoff: Thank you.

I can't comment with respect to the Amanda Todd case because, as you know, the British Columbia Attorney General has laid charges in relation to that case in respect of a person in the Netherlands, so that's an ongoing investigation.

The other part of your question was around what the United States or other countries have to assist them that we do not have.

Specifically, Bill C-13 would enact a lot of investigative tools, things such as the preservation order, the order that says “do not delete this data until we come back with a production order or a search warrant to actually access it”. That is a power that the Americans have had for many years, for at least for 15 or 20 years. We don't have that power.

That's also a power created by convention in the Council of Europe, a convention that, as the Minister indicated, we have signed but not yet ratified, and we will be the last of the G-7 to ratify it, if Parliament passes this bill.

Other provisions that would assist would those allowing the obtaining of transmission data. Basically that's data not with respect to the actual content of an e-mail, but one where it was sent, the route it took going through Rogers, through Bell, through Telus, through AT&T, going from the sender to the person who received it.

In the case of a cyberbullying situation, you have an e-mail that is received by the potential victim, and let's say that e-mail was part of the Bell network. You go to Bell network and Bell network says, “Well, that came from Rogers”. And then Rogers says, “Well, we were just a link in the chain. It came from AT&T”. Then you have to go to AT&T and say, “Well, are you their end point?”, and AT&T says, “Oh, no. That came from another service provider”.

These tools would enable the police to have all these ISPs preserve that data so that it's not routinely deleted, which is part of their practice, because they only hold it for a certain period of time. It would also allow them to get a transmission production order to say they're not asking for any of the content of the e-mail, but just want to know where the e-mail comes from. Did it come from across the street and go through all this routing, or did it come from another province or another country? That's all the police are asking.

Later on in the investigation, when they start to realize that maybe this were not just a suicide, that there may have been some criminality involved, that someone had encouraged someone else to commit suicide, then when they have a higher level of evidence and actually have reasonable grounds to believe, they can go to the ISP with a search warrant or a production order and say they now want to see the contents of the e-mail.

As the Minister said, it's a ramping-up system where at the first level, all you have is some suspicion that these e-mails might involve criminality, but you don't know that. All you want to do is to follow some leads, so you use the first tools to get the leads. When you get more evidence and you have more of a foundation for moving from suspicion to reasonable grounds to believe, then you start going after information that has a higher privacy standard, such as e-mail contents.

The Chair: Thank you very much for those answers.

Thank you for the question.

We are out of time.

Just so that the committee knows, next week we have four witnesses for our very first meeting on this. Two of them will be by video conference in the room that is available to us at 1 Wellington, so we'll be at 1 Wellington next week. Then on Thursday we will be back, I believe, on the Hill here with the Minister again for estimates, and then we'll be back to this study the week after that.

Thank you, by the way, to all the parties for providing their names, and we're working on putting the program together.

Thanks very much.

The meeting is adjourned.