HOUSE OF COMMONS
CHAMBRE DES COMMUNES
CANADA

Standing Committee on Justice and Human Rights

JUST • NUMBER 026 • 2nd SESSION • 41st PARLIAMENT

EVIDENCE

Tuesday, May 27, 2014

Chair

Mr. Mike Wallace

Standing Committee on Justice and Human Rights

Tuesday, May 27, 2014

● (1100)

[*English*]

The Chair (Mr. Mike Wallace (Burlington, CPC)): I'm going to call to order this meeting number 26 of the Standing Committee on Justice and Human Rights. As the orders of the day indicate, 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, is being discussed. We have a number of witnesses.

I am going to go over a few administrative things for the committee before we get started, ladies and gentlemen. First of all, here's what we have, based on the witnesses we've invited here, based on the suggestions from all parties. We have witnesses today and Thursday, and then Tuesday and Thursday of next week. Then I've set aside for the week after that two meetings at this point, Tuesday and Thursday, to deal with the clause by clause because I'm assuming that there may be a few amendments and some discussion on them. It could go faster than that, but we have set aside two meetings. So the clause by clause will start on June 10.

Obviously we can move motions on the fly, but I would really appreciate it if you could provide amendments by Friday, June 6, the week before the June 10 clause by clause so that they can be translated and circulated to committee members. That would be helpful.

I want to let you know that the organization Facebook is on a number of our suggested witness lists. They have indicated they're not that keen on coming. We've tried to schedule them and they get moved around and so on. Then they wanted to be represented by an Internet providers association, which is fine. All parties requested that we see Facebook, but I don't think we'll see them live. I think they'll be here by video conference, but at least they'll be here.

I would like to entertain a motion to re-invite them to make sure they understand that the committee really wants to see them on this issue.

Mr. Dechert.

Mr. Bob Dechert (Mississauga—Erindale, CPC): Mr. Chair, you took the words right out of my mouth. I was going to propose such a motion. They were on the NDP list, I believe, and the government list. We know Facebook as an entity and as a social media site was implicated in a number of cases of cyberbullying that we heard about last week, so I think it's very important that we hear from them. We should emphasize in our motion that all parties are requesting this, and we should compel them if necessary.

The Chair: Madame Boivin.

Ms. Françoise Boivin (Gatineau, NDP): I'm a bit surprised honestly, because they came and met with a lot of us and voiced their problems with the bill. It would be nice to hear them publicly and see what they propose. They see first-hand what's going on through their own site, and lots of kids are on the site, so I do hope that Facebook understands your message.

The Chair: So we have a motion moved that Facebook be re-invited, that all parties on the committee are interested in seeing them attend one of the remaining witness meetings that we have available, either this Thursday, or Tuesday or Thursday of next week.

I will make sure they get that message this afternoon, if the motion passes.

(Motion agreed to [See *Minutes of Proceedings*])

The Chair: Thank you very much.

Now we'll go to our witnesses. Thank you for indulging us in a little committee business. We have the witnesses and we'll do it as the list is presented here in front of us.

Mr. Gilhooly is here as an individual. From the Criminal Lawyers' Association we have Michael Spratt, who is a member of the association and criminal defence counsel. From the Canadian Bar Association, we have Marian Brown, executive member of the criminal justice section, and Gaylene Schellenberg, staff lawyer. And from the Kids' Network Safety Alliance, we have David Butt, who is legal counsel. I have a room full of lawyers today. It's a good thing we're at the justice committee.

Let's start with you, Mr. Gilhooly, as you're the first one on the list. You have 10 minutes.

● (1105)

Mr. Gregory Gilhooly (As an Individual): Thanks very much for having me. I consider it an honour to be here, and I have spent the past several weeks reading up on what the committee's been up to. I must say that as a citizen I'm encouraged by the way the committee is dealing with this as a political issue and not as a partisan issue.

It is sometimes trite to say that everything we deal with is politics, because it is, and the political process involves give and take and back and forth, with the result of reaching an end that serves everyone. Partisanship is something else when you are serving another end. To the extent that the written materials, the transcripts, indicate that this committee has been working in a political fashion and not a partisan fashion, I think that is to everyone's credit here.

Just for a quick introduction, I guess I am probably best known, unfortunately, as a victim of one of Canada's better known pedophiles, Graham James. I was in an approximately three-and-a-half-year relationship with Graham, and I came to the justice system as a victim when I decided to come forward with my story. I lived the tension that goes on in this room, because I'm also a lawyer. I'm a graduate of Princeton and then the University of Toronto Law School. I started my legal career at Torys as a corporate lawyer. I've served as general counsel at several companies. I'll get into that later when we start talking about the motivations that a company and legal departments may or may not have to voluntarily give over information.

Suffice it to say that going through law school as a victim was an interesting process. Sometimes we can get caught up in academic and very intellectual arguments when it comes to trying to parse exactly what can and can't go wrong with a piece of legislation. That's the proper process. You play things out to determine whether or not you are dealing with something that will fundamentally infringe someone else's rights. There is that delicate balance at play all the time.

I am not a “lock them up and throw away the key” type, but I must say at the outset that I commend the current government and this committee for the steps they seem to be taking to bring forth legislation of the type that we see before us in Bill C-13.

For full disclosure, I am a Liberal by political partisanship. I was a member of the Manitoba executive back when I was working with Canwest. I was a speech writer for David Matas, one of Canada's leading human rights lawyers. I consider myself lucky to have served the Liberal Party and lucky to have served David Matas, which may make some of the comments I'm going to make today in that context seem surprising, because I clearly live the tension—and you can probably see it as I rock back and forth in my chair—that there is the academic focus on preservation of individual rights and one's privacy, and there is the reality we face in our streets that there are monsters out there. When we sit down to write legislation or to take a look at legislation, we don't often consider the fact that there are monsters amongst us. I am living testimony to the fact that there are monsters amongst us. I have looked into the eye of the devil and have fortunately come out the other side.

I can say that we as a society sometimes, in my view, err in terms of ensuring that the rights of the individual are not sufficiently protected. I like to come at the issue from an approach that is opposite to what some of the people I assume will be speaking after me might take. I believe we have the wherewithal as a society to police behaviour and to ensure that our protectors are at all times acting in our best interests, and that if we ever find that the police or the state is going too far, that we as a society will take steps to correct the overreaching powers of the state.

I do not believe that anyone at any time need be afraid of legislating appropriate tools to protect children, to protect us, or to aid our police in trying to create a better society for all of us. If we make a mistake, we can always go back and correct it. We don't have to ratchet ourselves back at the outset in each and every instance to play against every hypothetical or every theoretical.

● (1110)

We live in a day where technology is changing. We are addressing cyberbullying here when we take a look at this bill, but we're clearly addressing more than simply cyberbullying. We are faced with any number of amendments to bring the Criminal Code into the now.

And to the extent that the police chiefs had issues with the tools at their disposal, my understanding in reading the transcript is that they made that clear to the committee earlier this month.

To the extent that victims welcome new legislation to protect others against things they have gone through, we heard from victims earlier this month as I read in the transcripts. I thought that Amanda Todd's mother was particularly brave in coming forward with her statement that she didn't want Amanda's name to be used as an excuse or an inroad to take away other's privacy rights. But at the same time, she was advocating tougher tools for the police. You can't have it spelled out any more clearly for you than the fact that there is a delicate dynamic: the balance is going to tip one way or the other eventually.

My concern as a victim is that the police have enough tools at their disposal to adequately protect us. My concern as a lawyer is that privacy rights and personal rights aren't trampled on. My reading of the bill here is that, but for a few tweaks, it's a very good step in the right direction. To the extent that your questioning of the police chiefs guided you in a way that gives you better tools and shows you how to craft the legislation properly, I think you're headed in the right direction.

I found it interesting in reading the transcript that, I guess, David Fraser came in. David is a leading practitioner in the field of privacy law. To say that I agree with everything he said I think would be an overstatement, but he is a bright man and he gave, I thought, excellent testimony to you to take under consideration.

What I found most fascinating, though, was when you move from the theoretical of David's testimony and into the practical examples that Mr. Dechert gave. You could see a breakdown in how theory didn't really mesh with what was going on in the real world. At one point when considering what appears to be one of the more controversial aspects in the legislation—the giving of information on the voluntary request when you're not otherwise prohibited from doing so—Mr. Dechert gave the example of a service provider who faces an emergency and you don't have time to get the warrant. The lawyer's answer was, “I would hope that the service provider would do the right thing.”

The unfortunate reality as a corporate lawyer who heads up a legal group is that you can hope all you want, but what the internal legal department is going to be saying is that there's not a chance unless we are clear that you are able to do that.

And so the interesting phenomenon we have in that one provision that seems to be taking up a lot of your time—although I'm focusing on it in the outset—is that the language appears to be a recasting of what is already present in the common law. Why does it have to be there? It's lawyer candy to say that if it's already the law, you don't need it to be the law. Well, there's clearly a problem, because you do need to remind people of their rights and their ability to do the right thing at the right time.

The way that the provision is crafted, it's simply there to remind corporate lawyers like me that you have the ability to do the right thing, and if you do the right thing you're not going to face repercussions from doing it.

I think there could be a slight tweaking of the language. To get technical for a bit—and I don't want to take too much of your time—there's the not prohibited language. The provision is cast so that you're able to give up information that you're not otherwise prohibited from giving up. Perhaps if you changed the concept from not otherwise prohibited or not prohibited to lawful—you're lawfully able to give up—that would be a slight tweaking.

But for that, I think you've got in front of you a bundle of proposed legislation that gives the police adequate opportunity to do the right thing in our society going forward. They need the tools. They've clearly shown a request for appropriate tools. The victims have spoken, and along the way in trying to balance rights and access and tools you're going to offend everybody.

So my hope is that you just continue to go ahead and do the right thing: offend all of us, but make sure that the crimes don't happen on a go-forward basis.

● (1115)

The Chair: Thank you very much for that presentation.

From the Criminal Lawyers' Association, we have Mr. Spratt.

Welcome back to the committee. The floor is yours.

Mr. Michael Spratt (Member and Criminal Defence Counsel, Criminal Lawyers' Association): Thank you. It's always a pleasure to be here.

As you may know, the Criminal Lawyers' Association is a not-for-profit organization comprising more than 1,100 criminal defence counsel from across Canada. One of our objectives is to educate not only our membership but also the public on issues relating to criminal and constitutional law. The CLA has routinely been consulted and invited by various parliamentary committees to share its views on proposed legislation pertaining to these issues. The CLA supports legislation that is fair, modest, constitutional, and supported by the evidence.

To cut to the chase, the CLA is simply unable to support Bill C-13. Quite simply, Bill C-13 is not only overly broad but is also likely unconstitutional.

Bill C-13 purports to be concerned with tackling cyberbullying by stopping the spread of intimate images that are disseminated without the subject's consent. The real tragedy of Bill C-13 is that those provisions are necessary, laudable, and should be proceeded with; however, in reality that aspect takes up only a small percentage of the bill. Bill C-13, in the balance, sacrifices privacy in favour of expanded police powers and liberal disclosure standards.

Bill C-13, along with Bill S-4 and Bill C-31, represents a dangerous and in our opinion unconstitutional pattern of erosion of privacy.

Let me speak of the cyberbullying provisions. They are important, are laudable, should be proceeded with, and are indeed necessary in the modern world that we live in. Largely, I don't have any objection to the small percentage of the bill that deals with those provisions.

Having said that, I would add that there is a legitimate argument that those provisions in and of themselves may be overly broad, in that the standard imposed for the *mens rea* is "recklessness". That standard of recklessness may go too far, in that it may make individuals potentially liable who don't know or could not have found out the circumstances to which the images that are the subject of that provision relate. To that extent, the problem with the cyberbullying provision is not necessarily its aim but rather its execution in that one small regard.

The bill's aim is to punish those who transmit intimate photos sent to them, when the person who took those images has an expectation of privacy. That is likely to have significant public support, as it should; however, the scope of the provision is potentially overly broad, because it expands the *mens rea* element. By making "recklessness" one of the potential *mens rea* standards for that offence, the provision may catch not only the individual who was the original recipient of the image but also those down the line—the second-hand recipients of that image—who may have no knowledge of the circumstances in which that picture was taken or made.

Some caution comes from Don Stuart, a pre-eminent expert in the field of criminal law. As he points out in *Canadian Criminal Law*, the fifth edition, there is a risk that the recklessness standard can devolve into a far broader conception of fault than is desirable, and a more nuanced approach would involve defining recklessness as knowledge both of the risk and that that risk was likely.

That provision can be seen in other aspects of the code; for example, in item (a)(ii) of section 229, which deals with murder.

A modified recklessness standard in the cyberbullying provision would target the so-called "revenge porn" conduct, without drawing to the net those who simply pass on the photos without context and may not necessarily be as morally culpable.

If the provision is allowed to remain there without a clearer definition of recklessness, the section may attract some charter scrutiny. At that point, the issue would become one of over-breadth: does that section capture individuals who may not be morally blameworthy, but may nonetheless be captured under the recklessness standard? As I said, this is a minor issue with that aspect of the bill.

More troubling is the "lawful disclosure" aspect of Bill C-13. The bill announces itself as being about cyberbullying and protecting Canadians from online crime, but certainly it far exceeds those parameters.

I will start by saying that of course the most controversial aspects of Bill C-30 have been removed—the mandatory warrantless disclosure of basic subscriber information. However, there are still some serious concerns. I'll deal with two issues.

The first is that there is simply insufficient judicial oversight in obtaining those orders.

● (1120)

Now, the Supreme Court of Canada has recently considered the standard for reasonable suspicion, which is the standard we're dealing with in the legislation, in the case R. v. Chehil. The court made it crystal clear that the standard of reasonable suspicion falls well below the normal requirement of reasonable and probable grounds. That's the normal standard we usually deal with. Specifically, the Supreme Court said that the state's interest in detecting and preventing crime begins to prevail over the individual's interest in being left alone at the point where credible-based probability replaces suspicion.

The data, which is the subject matter of the searches contemplated in Bill C-13, contains a great deal of personal information. It's a misnomer to simply call it metadata. That dilutes the importance and impact of that data.

I understand that a pre-eminent expert in this area, Dr. Michael Geist, will be testifying at this committee later this week, and I think he will agree that metadata is deserving of an increased level of protection. And indeed he's not alone in that view. When we look at reports in 2013 from the Information and Privacy Commissioner of Ontario and the Office of the Privacy Commissioner of Canada, both reports reveal the heightened expectation and the intimate information that can be revealed through metadata. I would commend you to read those reports. It's quite shocking what can be discerned about an individual's communications and basic information about the individual through simply an IP address or some of the other metadata that's discussed.

Metadata as a starting point has a heightened expectation of privacy, and that is something that has been echoed by the Supreme Court, which agrees seemingly with Dr. Geist and with the privacy commissioners. In the recent case of Vu, which dealt with metadata found on a personal computer, the Supreme Court of Canada adopted the Criminal Lawyers' Association's submissions—we intervened in that case—finding that ordinarily this information, metadata, can help a user retrace his or her cybernetic steps. In the context of a criminal investigation, however, it can also enable investigators to access intimate details about a user's interests, habits, identities, drawing on a record that the user created unwittingly. Of course, in modern times there's a capacity to store, catalogue, and cross reference this information, revealing more and more.

The Supreme Court's comments about the heightened privacy inherent in this type of data is simply incompatible with the proposed reasonable suspicion standard that's found in Bill C-13. That incongruity exposes this proposed legislation to charter scrutiny, and in my opinion supports a conclusion that there's not only charter scrutiny here but indeed charter infirmity. There's simply no principled and justifiable reason that the new warrant provisions contained in Bill C-13 should not be based on the traditionally and judicially approved standard of reasonable and probably grounds.

Next, moving to the issue of the incentives for non-judicially supervised disclosure, Bill C-13 will also likely lead to an increased request for a telecommunications company to disclose information without court oversight and the corresponding protections. Privacy in this regard should be strengthened and not abandoned. Falling back on section 25 in the current Criminal Code is no answer to this problem. If you read section 25 carefully, you will see that section 25 requires reasonable grounds, and no comfort can be found in the appeal legislation as it offers no protection.

Of course as we see with that existing provision in Bill C-13, it broadens the scope of disclosure. No longer will the requesting organization be under an obligation to actually be enforcing or administering an act. The room for those requests is greatly increased. And indeed we see codification of the civil and criminal immunity which isn't in section 25, and as I said, section 25 requires reasonable grounds, which is completely absent in this section.

The real concern is that the expansion of police power and limiting liability for the party agreeing to disclose will result in increased police fishing expeditions, and of course we have seen from some reports some very alarming information about current practices in that regard.

● (1125)

Indeed, it would have been preferable to have discrete legislation on both the cyberbullying and on the lawful access legislation. However, given the current formulation of Bill C-13, the CLA recommends that the standards for obtaining those warrants be strengthened and brought in line with what the current Supreme Court case law would suggest is appropriate. No one wants to see evidence excluded. No one wants to get it wrong at the outset, and years later find out that the constitutionally suspect legislation was passed, evidence was excluded, and prosecutions were jeopardized because things weren't done right the first time. The provisions respecting the voluntary disclosure should be reconsidered to ensure both fairness, respect of privacy, and ultimately, constitutionality.

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

Our next presenter is from the Canadian Bar Association.

I'm assuming that Ms. Brown is leading that off, but you're both welcome to speak. Or is it Ms. Schellenberg?

Ms. Gaylene Schellenberg (Staff Lawyer, Law Reform, Canadian Bar Association): I'll just introduce the CBA briefly.

Thank you for the invitation to present the Canadian Bar Association's views on Bill C-13 to you today.

The CBA is a national association of over 37,500 lawyers, students, notaries, and academics. An important aspect of our mandate is seeking improvements in the law and the administration of justice, and it's that aspect of our mandate that brings us to you today.

Our submission on Bill C-13 was a joint effort, a team led by our national criminal justice section with input from our privacy and access to information law section, our competition law section, as well as our children's law committee.

With me is Marian Brown, an executive member of our national criminal justice section. That section's membership represents a balance of crown and defence lawyers from all parts of the country. Ms. Brown has practised criminal law in B.C. as crown attorney, as defence counsel, and as counsel for an oversight agency investigating police for over 18 years. She'll now address the substance of our submission and respond to your questions.

Thank you.

Ms. Marian K. Brown (Executive Member, Criminal Justice Section, Canadian Bar Association): Thank you, Ms. Schellenberg.

We hope that our input today will assist you in understanding how the draft provisions would function, if they're implemented, and of course in understanding what constitutional or charter issues may arise.

We are proposing numerous amendments that all have one of two main goals. Our first goal is to ensure that only truly intentional cyberbullying is prosecuted, and our second is to ensure that privacy interests are protected when data is seized.

Our written submission provides many details that we will not be able to cover today. What I will do now is give highlights of our recommendations on cyberbullying, on lawful access, and on the Competition Act.

First with respect to cyberbullying, as you know, the bill criminalizes a particular form of cyberbullying, which is the non-consensual distribution of intimate images. Distribution of sexual images of children is already prohibited by the child pornography provisions by the code, but the new section 162.1 proposed in Bill C-13 criminalizes non-consensual distribution of anyone's intimate images, not just young people's. In the CBA's view, this new offence is better suited to dealing with youth cyberbullying than using the child pornography provisions for youth conduct.

We're recommending some amendments that would more closely restrict the new offence to situations of truly intentional bullying. We echo Mr. Spratt's concern about the current wording of proposed section 162.1, which includes the alternative of recklessness. That could, in our view, criminalize conduct that is merely careless, and carelessness is an aspect of youth behaviour. Prosecuting someone who does not have the knowledge or intent required for a criminal offence would be a violation of section 7 of the charter.

In our written submission, at page 5 of the English version, we give an example of an adult distribution of images that would constitute reckless or careless conduct, but which is probably not the aim of this legislation. Because there are scenarios in which carelessness or reckless distribution under the current wording could incur criminal liability, we're recommending two specific changes to the wording.

Our recommendation 2, which appears at page 6 of the English version, is that the following phrase should be added to the offence section: “with intent to annoy, embarrass, intimidate or harass that person”. It's a much more specific formulation of intent. Our recommendation 4, at page 7 of the English version, is that the offence section be amended to remove the words “being reckless as to whether or not that person gave their consent”.

So we would take out the alternative of recklessness. In our view, those two amendments would ensure that only the distribution of images with a malicious intent would be prosecuted and would ensure that young people are not prosecuted for their merely careless or thoughtless distribution of images.

I'll turn now to our key submissions regarding lawful access. Seven of the eight main lawful access powers in this bill rest with the judiciary; that is to say that seven of those eight powers consist of judicial orders or warrants. The one exception is the preservation demand by an officer, whereby data is not seized without judicial authorization but is simply ordered to be held, so that it cannot be deleted, for a period of time.

So there is no warrantless seizure provision under this proposed regime, but the CBA recognizes that the issue of privacy in data is much broader than these particular Criminal Code seizure provisions. As we've heard from other presenters, perhaps the greatest concern is about law enforcement's obtaining data through the cooperation of service providers without the use of any of the eight powers that are covered in Bill C-13. Obtaining data outside of the Criminal Code purports to be authorized under PIPEDA, the electronic documents act, and other privacy statutes.

● (1130)

We feel it's important to comment that even if the lawful access provisions in Bill C-13 are made perfect, this will not eliminate arguments that PIPEDA and the other privacy acts perhaps should be more strictly applied. Even the very best drafted Criminal Code provisions will not diminish the arguments that voluntary cooperation between service providers and law enforcement should be more closely monitored.

Because of that bigger picture, two of the CBA's recommendations are quite broad. Our recommendation 8, at page 12 of our written submission, is that a single entity be created to monitor the impact of the seizure, retention, and use of personal information by Canadian law enforcement agencies.

Our recommendation 17, at page 24 of the English version of our written submission, is that the federal government conduct an independent comprehensive review of privacy interests in the context of electronic investigations.

Those sound very broad, but we're in a new world here. We're at a perfect storm of legal change and technological change, and it's no wonder that we're having difficulty with it.

Given the bill that you have to work with today, in our written submission we make several specific recommendations for amendments. We believe that three amendments in particular are key to avoiding violations of privacy interests under section 8 of the charter.

Our recommendation 9, at page 14 of the English version of our written submission, is that the officers' preservation demand, which is section 487.012—the only power without judicial authorization—should be limited to exigent circumstances, where data would otherwise be lost or destroyed before a judicial authorization can be obtained.

Our recommendation 14, at page 19 of the English version, is that the threshold for a transmission data production order—and that's section 487.017—should be raised from "reasonable grounds to suspect" to "reasonable grounds to believe" because transmission data may reveal private conduct.

Similarly, our recommendation 15, at page 20 of the English version, is that the threshold for a transmission data recorder warrant, section 492.2, also should be raised from "reasonable grounds to suspect" to "reasonable grounds to believe", again because transmission data may reveal private conduct.

I'm going to say a few more words about transmission data. Our understanding is that it's not the same thing as metadata, which we understand to be data left by web browsing that can be located on a personal computer that is seized under a search warrant. We understand transmission data, as defined in this bill, to include not the contents of the communication, but only its origin and destination, direction, duration, time and date, size, and the protocol and type of the communication. That limited definition is very important because intercepting the contents of a private communication actually is a criminal offence under section 184 of the Criminal Code, unless a wiretap authorization is in place.

Bill C-13 cannot entail monitoring of the content of private communications.

I don't want to overlook the so-called immunity section, but unfortunately our working group did not discuss it in detail or make written recommendations about it. You've heard from other speakers about the terms of that section. All we can recommend is that you look closely and comparatively at the proposed section 487.0195, the existing section, which is old number 487.0114, combined with section 25 of the code, and you may wish for comparative purposes to also look at the immunity provision that exists for people who voluntarily assist with wiretap orders, which is section 188.2 of the Criminal Code. You'll see in that section that there is full civil immunity only for people who assist where there is either a judicial authorization or an interception in exigent circumstances. It's a more limited option for immunity.

● (1135)

The Chair: Wrap it up, please.

Ms. Marian K. Brown: I will.

I just want to make a very brief comment about the Competition Act provisions, which are generally overlooked. We do have a recommendation that clause 29, creating a new section 14.1 of the Competition Act, should be deleted. The section would import Criminal Code preservation orders and production orders into the non-criminal reviews of the Competition Bureau. We maintain that Parliament's original attempt with the Competition Act was to have two distinct processes: one for criminal investigations and one for administrative review, and criminal procedure should not be imported into the administrative review process.

The Chair: Thank you for that presentation from the Canadian Bar Association.

Our final speaker this morning is from the Kids' Internet Safety Alliance.

Mr. Butt, the floor is yours for 10 minutes.

Mr. David Butt (Counsel, Kids' Internet Safety Alliance - KINSA): Thank you very much. It's a great pleasure for KINSA to be asked to present.

Just briefly, KINSA, the Kids' Internet Safety Alliance, is a Canadian not-for-profit with a global footprint whose mission is to save and protect children everywhere around the world from Internet-based child exploitation.

My background is as counsel to KINSA. Before that I was a founding board member who served on the board for a number of years. In my non-volunteer life, I'm a criminal lawyer, and have been for 25 years. Right about now, I'm at the point where I've spent about half the time prosecuting and half on the defence side, so I've been on both sides. I'm currently in private practice.

A significant component of my practice is representing victims of crime when they require independent counsel to advance their interests in criminal prosecutions. A third aspect of my practice, and it's a three-cornered practice, is representing police officers in all manner of professional discipline and review and policing issues that arise. So I like to say I've touched all the bases in the criminal justice system in my 25 years. Coincidentally, this past year I've also just reached 25 cases that I've litigated in the Supreme Court of Canada. Unfortunately, on the last one I got my butt kicked—

Some hon. members: Oh, oh!

Mr. David Butt: —and I can say that with my last name. I know what it's like to litigate these issues constitutionally.

So speaking on behalf of KINSA, I bring that practical perspective of a front-line criminal lawyer and ask the question, how does this stuff work? For me, looking at it from both sides, here's the key. I think Greg has really hit the nail on the head that you're going to have the tension between privacy and effective law enforcement. There are three ways to respond, and two of them are wrong and one of them is right—and I say, you have the third way, which is right, in this bill.

The first way that's wrong is to not give police powers because you're afraid to give them powers. That would be wrong because I think the Canadian community rightly expects that police will be able to conduct sophisticated and effective investigations in a digital world. I think that's a baseline expectation.

The other thing to do wrong is to ignore privacy. I think that Canadians expect that while police are conducting effective digital investigations they will be according appropriate respect to privacy. So another wrong way is to just ignore the privacy piece.

The right way is to ask the this question: let's have vibrant police powers to investigate digitally, coupled with significant judicial oversight to control those police powers independently. That's the sweet spot that I say this bill hits. That's my measure of success in a bill: does it enable the police to act effectively, but does it also give another branch of government, the judiciary, the appropriate tools to oversee? If you've got both of those, you've got the right mix, and I say you've got the right mix here.

Let me just talk to a couple of specific things people have mentioned this morning that I take a different view on, because of that basic view I take of the bill.

First, in regard to the recklessness standard, appellate courts have written pages and pages on the definition of recklessness. 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. That's a standard I hold my 10-year-old to. If they never thought of it, fair enough. That's why I agree, we can't have a carelessness standard. But a recklessness standard, you turned your mind to the possibility and you went ahead anyway. Recklessness, in my view, in the context of the distribution of these intimate images, is an appropriate standard.

Second, in regard to reasonable suspicion, our Supreme Court of Canada said in 2004 that the police can exercise powers based on reasonable suspicion. So let's not have any misconception that reasonable suspicion is somehow constitutionally problematic. Police officers, as found in cases like R. v. Mann, can detain people based on a reasonable suspicion.

● (1140)

So, if I as a uniformed officer can grab you and hold you based on a reasonable suspicion, why can't I ask a judge to approve the seizure of minimal data that will simply give you enough to get a proper warrant to do the investigation? It's not carrying the whole investigation; it's only getting you in the door so that you can then get a warrant. So I say reasonable suspicion is appropriate in these circumstances, and it's limited to certain things.

As for anything that goes to the content of the conversation, as I read this bill, you have to get a full-on warrant with reasonable grounds. If transmission data, as I read it in this bill, is simply stuff that will allow you to identify where you need to go to get a warrant, I say that's fine. And if the experts on transmission data say that's a broader problem, I defer to the experts

The other thing is that those who have objected to transmission data and to reasonable suspicion, I say, haven't taken into account the protections that you have wisely built in. For example, if I get a reasonable suspicion-based production order as a company, I don't have to comply. I can go to a judge and I say, “This is way too broad. I'm not going to comply.” The judge can hear and can weigh it. There's no downside other than emasculating the police getting the data they need. So that's a crucial aspect that will address any concerns about over-breadth.

As for the immunity provision, it says that you're okay if you turn over stuff you are already able to turn over. As Greg so rightly said, “Why do we even need it?” It's a reminder to foster industry cooperation. Who is going to decide what is okay to turn over? It's not up to the police. It's not up to the companies. Guess what? It's up to the courts. They're the protectors of the Constitution. They're the ones who say what you can lawfully turn over.

There's a very interesting point that I think hasn't yet come into the conversation: what do the courts say? Based on a case called Ward, out of Ontario, and the Spencer case that was heard in December in the Supreme Court, which is probably coming out soon, the courts say right now that all you can ask for is basic subscriber name and address information. It has to be in the context of a specific investigation, narrowly tailored. It cannot be a fishing expedition. And it has to take into account what the acceptable-use policies of the provider of that information are. Most responsible corporate citizens have acceptable-use policies that say, “We're not going to let you use our service to hide from criminal activity.”

So the courts look at all of those things, and what you can ask for lawfully in a criminal context is very narrow. So on that provision that says you're okay giving up what's already lawful to give up, I would point out the following, first, it's redundant; second, it sends a great message of cooperation; and third, the courts have already defined it narrowly, because what may lawfully be given up is up to the courts. For all those reasons, I say, you're on the right track.

Thanks.

● (1145)

The Chair: Thank you for that presentation.

We'll now go to questions and answers.

Our first questioner is from the New Democratic Party. It's Madame Boivin.

Ms. Françoise Boivin: It's interesting to see so much diversity of opinion, which is not making our job any easier.

[*Translation*]

Rather than debate with you myself, I will let you debate one another. That will probably make things a bit more interesting.

I get the sense that the two people in the middle are somewhat of the same mind as I am, and that the two at the far ends—not to suggest that your views are as far out as your seats, of course—have a different opinion.

Mr. Spratt and Mr. Brown, I'd like to hear how you respond to Mr. Butt's arguments on the issues of recklessness and reasonable suspicion and on the immunity provision. How do you respond to what he just said? His comments would suggest that the bill is reasonable. I'd like to hear both of your takes on that.

I have a concern about Bill C-13 that no one has brought up. The whole matter of warrants makes us think that people's personal information will be passed around without their ever knowing about it. I haven't seen any amendment or provision being proposed to address that. I'd like to hear your thoughts on that issue.

Thank you. Fill your boots.

[*English*]

Mr. Michael Spratt: In addressing some of the points that Mr. Butt raised, I think it's a bit of a straw man argument to say that requiring stricter controls somehow emasculates the police. I mean that's simply untrue. Of course, if there are exigent circumstances, the police don't need a warrant. If there are exigent circumstances, the police can enter your house without a warrant. So let's leave that aside. The police can also request that information be preserved. The police have that ability as well.

I think the biggest difference lies in the underappreciation of Mr. Butt's part of the type of information that is to be disclosed. Certainly, privacy commissioners and academics disagree with the narrow view of the type of information that can be disclosed. The Supreme Court has taken a view that this sort of information deserves a heightened level of privacy.

If you look at the report, it's not just simply saying that person X is the person who is operating that computer. That information can be catalogued, can be stored, can be cross-referenced—and that only increases as capacity grows—but that information can, for example, lead to information about which websites you visited and what posts you've made. In one case, it allowed—and this is in the Privacy Commissioner of Canada's report—a determination based on websites visited, sexual preferences, and political affiliations. It's not just who you talk to, it's who they talk to and for how long. The fact that content isn't available is no shield to the criticisms here.

As the Information and Privacy Commissioner of Ontario said, in some respects, and in many cases, metadata is actually more revealing than content. So it's a straw man argument to say that this somehow emasculates the police, and that they can't do their job with the standard that is constitutional. What nobody wants to see—and we have seen a few times in the last little while—is that constitutional issues arise, as in R. v. Vu. In that case, evidence was excluded and prosecutions were affected. Ultimately, the matter didn't make its way through the courts. The extra burden to require reasonable grounds is a requirement in section 25. Section 25, and the protections against voluntary disclosure, make it clear that there have to be reasonable grounds. With the ability to preserve the data, there is no principled reason why a standard of reasonable and probable grounds shouldn't apply with this type of information. The police still have the tools, and privacy is still protected that way.

● (1150)

The Chair: I'll go to Ms. Brown for an answer as well.

You have two minutes.

Ms. Marian K. Brown: Okay.

We don't see a provision here that concerns metadata from web surfing. To our knowledge, that kind of evidence is obtained by seizing a computer and forensically examining it, and that is well covered by other law outside of this bill.

With respect to the standard of recklessness in the offence provision, the word “knowingly” appears twice in the provision. In criminal law, the word “knowingly” includes wilful blindness, and that is the standard that we would like to see. Wilful blindness occurs when one knows that there was probably no consent to distribution of the image, but one goes ahead anyway. It's a higher standard of knowing that there was probably no consent. The word “knowingly” alone imports that concept of wilful blindness.

With respect to reasonable submission, you've heard from other witnesses how that standard applies to the earlier stages of an investigation where there is a lower expectation of privacy in the data, for example in—we would say—transmission data. We totally agree that the higher standard of reasonable grounds should apply to the later stages of an investigation, and with material for which there is a greater expectation of privacy.

Under these provisions, with respect to the lack of public knowledge of what data is seized, production orders and warrants are all obtained by means of an information to obtain, ITO, the order or warrant. The information to obtain may be dozens of pages long, or hundreds of pages long, and is filed in the court registry. There is a presumption of public access, although there may be a sealing provision for the duration of the investigation. For these judicially authorized measures there is an enormous public record, but we agree that public knowledge of how information is subsequently retained is a problem area. People do not know what happens to their data after an investigation has concluded. There is simply no provision for that in either the existing code or in the amendments.

The Chair: Thank you very much for those questions and answers.

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

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

Thank you, each of our witnesses, for being here today.

My time is short, so I'm going to move fairly quickly through these questions.

Mr. Butt, both you and Mr. Gilhooly have, I think, effectively made the case about the so-called indemnity provision. I just wanted to see if I can get you to clarify that. We're talking about proposed subsection 487.0195(2) of the bill.

A lot of people say this opens up new law, or this creates new law, and it gives the ISPs the opportunity to provide much more information than they have in the past and to escape any civil or criminal liability for doing so. Do you think that provision changes the law at all from the current standard, including the case law?

● (1155)

Mr. Gregory Gilhooly: No.

Mr. David Butt: No.

Mr. Bob Dechert: Thank you very much.

I think you both have taken us through the recklessness standard and some of the other key provisions of this bill, and you both mentioned that there's a tension here. Clearly what we're all struggling with is that we need to draw a line between protection of privacy and prevention of harm.

Mr. Gilhooly, you said in your opening comments that if we make a mistake, we can always go back and correct it. What harm is there if the ISP provides the name and address of someone who may be sending an image or sending a message that the party on the other side thinks is bullying but that may turn out, when looked at judicially, not to be? What is the harm to the person whose information is being disclosed versus the need to act quickly to prevent the harm, if in fact it is a case of criminal liability? Can you speak to that, Mr. Gilhooly, as a victim and as a lawyer?

I'd like to hear from Mr. Butt as well.

Mr. Gregory Gilhooly: There is almost a difference between policing and prosecution, when you get down to thinking about it. We have some very technical arguments here about how to ensure the legislation complies so that we can end up with charter-proof prosecutions of criminals.

I'm, firstly, worried about keeping our children and citizens alive, when it comes to the issues of cyberbullying. So I want to ensure that the police have the tools to intervene and do whatever they can to stop the crime. If it turns out that our laws have gone too far in accordance with what the charter sets out, I'm more than happy to have a perpetrator walk but to have a child alive. I know that's a somewhat trite thing to say, but as victims, we want to see laws that protect society. We, as victims, don't want to see rights trampled, but the tie has to go to the victim here. Unless the statute is egregious in its trampling of privacy rights, my hope is that we're going to err on the side of giving the police the appropriate tools to intervene.

Mr. Bob Dechert: Do you see any egregious trampling of privacy rights in this bill?

Mr. Gregory Gilhooly: No.

Mr. Bob Dechert: Mr. Butt, do you have a view?

Mr. David Butt: In terms of "what's the harm?", I wrote about this in *The Globe and Mail* a couple of weeks ago. It's a short example that makes the point.

KINSA works directly with police officers to devise training on Internet child exploitation investigations that we can deliver in developing countries. We have a lot of experience working closely with police officers. So I asked one of our instructors what the difference was. "Why shouldn't they have to get a judicial order for everything? Why can't they just request basic names and subscriber information?" He gave me a great example, which I stole and put in the paper. It's this.

Sally is bullied. She opens her email, and there's a horrific bullying message from some anonymous person, just known as "Bully Dude". I asked the police officer this. The family is upset, and they want immediate action. If you could call and get just the basic subscriber information, how long would it take before you could start working on a warrant to actually investigate? He said it would take minutes. I asked him how long it would take to do judicial production orders just to get the basic subscriber information. He said they'd have to draft it and get it judicially approved. It would go into the busy Internet service provider's inbox with a ton of others. It could sit there for 30 to 60 days. That is just for the basic subscriber information.

I say let's give that information. It's just a bit of information that allows the police to say, "Here is the person against whom we want to do a full warrant." That's all it does. And they proceed from there. It's minutes versus 60 days. That's an appropriate trade-off, in my view.

Mr. Bob Dechert: Ms. Brown, do you have a view on where you draw the line between protection of privacy and prevention of harm, and what is the potential harm of disclosure of the information to the police if they're trying to prevent harm, as Mr. Butt just mentioned ?

Ms. Marian K. Brown: Subscriber information?

● (1200)

Mr. Bob Dechert: Correct.

Ms. Marian K. Brown: Well that issue is squarely before the Supreme Court of Canada in the Spencer case. So I'm waiting to hear what they say. It's been very well argued both ways that subscriber information is either like name and address information, or that it's the crucial link that enables determination of core biographical information, charter protected information—

Mr. Bob Dechert: Let's say that wider amount of information was disclosed to the police in error. What's the harm to that individual?

Ms. Marian K. Brown: Disclosed to the police in error, unlawfully?

Mr. Bob Dechert: Unlawfully, the courts have determined too much information was disclosed, what is the harm to the subscriber in that case? Can you give us information on that?

Ms. Marian K. Brown: Yes, infringement of a charter protected privacy interest is a harm. Privacy is something that we value in our justice system and to infringe someone's privacy in those circumstances weakens the protection of everyone's privacy in general.

Mr. Bob Dechert: How do you balance that against the need to move quickly to protect a young victim in a case like for example with Rehtaeh Parsons or Amanda Todd?

Ms. Marian K. Brown: If you're asking about non-judicially authorized disclosure, that is currently made under the provisions of PIPEDA or the privacy acts and there's a great debate whether those provisions are tight enough. That goes beyond what we can deal with in Bill C-13—

Mr. Bob Dechert: Does anything in Bill C-13 change PIPEDA?

Ms. Marian K. Brown: No.

The Chair: Thank you very much.

Next from the Liberal Party is Mr. MacAulay. Thank you for joining us today.

Hon. Lawrence MacAulay (Cardigan, Lib.): Thank you, Mr. Chair, and welcome to the witnesses. Your presentations were excellent.

I have a question for Mr. Spratt.

On May 1, this committee heard my colleague from the Liberal Party question the Minister of Justice on the proposed subsection 487.0195(2). The minister said this section 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.

He also said its purpose is also to spell out more clearly 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, this is a re-enactment of that existing section. So it is there for emphasis.

When my colleague asked the minister if he agrees that Bill C-13 codifies an immunity for telephone companies from class action lawsuits when they cooperate with warrants, with lawful demands for documents, the minister responded by saying that if it is deemed lawful, then they should be immune from prosecution and that 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.

Finally, when my colleague asked the minister about the circumstances where you have a warrantless but lawful request made by law enforcement to a telephone company, whether he agreed that in those circumstances the telephone companies had no obligation to disclose to their subscribers that they have given this information to authorities without a warrant lawfully, the minister said 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. It must be done in a way that complies with section 25 and this other section, 487.

Mr. Spratt, can you comment on the responses by the minister and do you agree with what the minister had to say?

Mr. Michael Spratt: I don't agree. I think a reading of the legislation would logically lead one to that conclusion.

The minister said that the obligation to disclose to an individual when their information has been disclosed was covered under PIPEDA. It's not. It's quite clear, when you look at PIPEDA, that subparagraph 7(1)(c)(ii) doesn't require that there be any disclosure to the individual.

When the minister says that it must comply with section 25, that's simply not accurate when you look at the text of section 25, which requires that the person disclosing “acts on reasonable grounds”. And reasonable grounds isn't just asking for the information—“I need this information for an investigation”—and then having the telco comply and give it to you. That's not reasonable grounds. If reasonable grounds is required for the protection of section 25, the case can be made to a judge.

It's not the case that this hamstrings investigations. In my experience, in the case of some of the tragic examples that this committee has heard, it's not the case that it would take 30 to 60 days to retrieve that information. That's simply not how it works.

The section that the minister was speaking of broadens the ability to ask for that information. Certainly combined with other bills, such as Bill S-4, it raises severe privacy concerns in terms of the broadening of that information. It's not consistent with section 25, which requires reasonable grounds.

In fact, the countless hundreds of thousands of example that we've heard about over the last month about this sort of voluntary disclosure is troubling, and this does nothing to address that. It does nothing to address notifications to persons affected.

What's the danger with people asking for this information? I'm sure you've all read the stories about record checks, police checks, state storage of information, disclosure of that information.That's the danger. It's not an answer to say that if you have nothing to hide, you should be willing to give this information over. What's the harm? The harm is done when the charter is breached. That's the standard. The tie doesn't go to the victim. The tie should go to the charter, which is the supreme law and should be respected.

Privacy is not about hiding. It's not about secrecy. Privacy is about a person's right and ability to control the information about them and their freedom of choice. Just as I have a privacy interest in my voice when it goes through the telephone lines at the telecommunications companies, I also should have, and citizens should have, privacy interests in other data. It's a misnomer to say that the legislation makes it clear that this just subscriber data, i.e., name. That's not what it says. It's the type, duration, date, time, size, origin, destination, and termination of your data and anyone else's data.

When that net is cast, I say there's not even close to a tie here. The police aren't hamstrung. They can take the appropriate steps and we can be protected. Police can do their job, and at the same time, we can respect not only individuals' privacies but also comply with the strict standards that we're entitled to under the charter.

● (1205)

The Chair: You have one minute left.

Hon. Lawrence MacAulay: Thank you very much.

The minister and department basically refused to talked about the combined effect of Bill S-4 before the Senate and the bill before the Senate committee. Should Canadians be concerned about this issue?

Mr. Michael Spratt: Yes. What we're looking at under PIPEDA is that with regard to the information disclosed for the purposes of law enforcement, there's no necessity to disclose to the person who you're talking about, who the information pertains to. Bill S-4 takes it a step further, of course, and says it's not just law enforcement or the government, but it's other organizations as well. We see in Bill C-31 that no longer are there strict controls over the sharing of information between Revenue Canada and other organizations.

This is a pattern, and it's a concerning pattern. To that extent, if would be very useful if this issue could be studied in depth in relation to the other issues that impact it as well.

The Chair: Thank you very much.

Our next questioner is from the Conservative Party.

Monsieur Goguen.

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

Thank you to all the witnesses. That is certainly a probing and in-depth analysis of this legislation. It's pretty clear that the debate is about balancing the protection of the public and, of course, the protection of privacy.

Everyone knows that on the Internet now everything acts lightning fast, so the balance, of course, has to be tempered with the ability to react rapidly. Of course getting information for a warrant takes so much time that it's often not possible to get the information before it's deleted, and therefore that hampers the police.

I came across a very interesting article. This was in the Canwest News Service. I'm not accustomed to reading out these things, but this is very telling. It was from March 12, 2009 and it's basically an article based on data that has been gathered by Cybertip.ca—which, of course, the federal government subsidizes—and it's much in tune with what Mr. Butt does. I'm sure you're aware of this organization.

The article says the following:

> Canada's first statistical portrait of Internet child-luring tells a story of police who are losing the battle to catch cyberspace predators, and judges who are unlikely to jail the few who end up in court.
>
> Statistics Canada reported Thursday that two out of...three cases are never solved, and the vast majority of luring is never reported in the first place.
>
> Even when the suspects are charged and the perpetrators convicted, courts are more likely than not to spare them jail time, said the data-collection agency.
>
> The first analysis of the seven-year-old Criminal Code offence concluded that the police track record in solving the borderless crime is worsening as technology advances—and children are, increasingly, living their lives online and offering up personal information that makes them easy prey.

The numbers are as follows: Cybertip.ca received a total of 21,000 tips about online child exploitation between its launch in 2002 and January 2008. Ninety per cent of the tips were about child pornography; eight per cent of the tips were about online child luring; one per cent of the tips were about child exploitation through prostitution; and one per cent were about child sex tourism.

So let's talk about the tie. Should the balance not go in favour of the police, who are trying to obtain information to protect children by using minimal intrusions into privacy, or should it go to the privacy of the people who are offending?

● (1210)

The Chair: Are you asking someone specifically?

Mr. Robert Goguen: That's for Mr. Butt or Mr. Gilhooly.

Mr. David Butt: I'd like to cast the question a little bit differently. I think this bill is a win-win because it has extensive judicial oversight that minimizes and regulates intrusiveness of the police. The very narrow area in which Internet service subscribers can voluntarily turn over will be defined by the courts. For example, we're waiting for the case of Spencer to come out of the Supreme Court of Canada. If the Supreme Court of Canada says “no subscriber information”, guess what? You don't have to amend this bill. You can't give it any more.

Mr. Robert Goguen: Every law goes through a cycle. The cases interpret the law, and of course the bill to jurisprudence.

The last time I checked we weren't living in a police state.

Mr. David Butt: The courts are very much alive as to what you can turn over voluntarily, and all the rest requires prior judicial authorization, so I think that's a win-win. I don't think it's a tie and you pick a winner. I think that our privacy has robust protections in this bill, all of which are supervised by the court, and of course the provisions that enable law enforcement to move more effectively address those very serious criminal misconduct issues that you've identified.

Mr. Gregory Gilhooly: Just to pick up on that, when we talk about a tie going one way or the other, we're not talking about one side having charter rights and one side not having charter rights. Remember, Rehtaeh Parsons had charter rights to live a secure life. The criminal gets involved in the situation with or without rights.

We're talking about a delicate balancing of all rights, and victims have rights, too. That's one of the things that are increasingly coming up now as legislation is introduced: Victims are a part of this process as much as perpetrators are. Those victims have rights, and those victims' charter rights deserve to be heard, respected, and considered in the legislation that you are considering at all times.

Mr. Robert Goguen: In fact, when victims are victimized, their privacy is invaded as well, so there is a trade-off there. It's much in tune with what Mr. Butt is saying that it's a bit of a win-win. You should be able to shelter yourself from criminal activity under the auspices of privacy, surely.

That's all I have, Mr. Chair.

The Chair: Okay, thank you very much.

Our next questioner, from the New Democratic Party, is Madame Péclet.

[*Translation*]

Ms. Ève Péclet (La Pointe-de-l'Île, NDP): Thank you kindly, Mr. Chair.

[*English*]

Thank you very much to all of the witnesses.

Before I start, I want to make it clear that this is not about police officers and it's not about the courts. It's about having the best legislation.

Thank you very much for all your input. You're all brilliant minds and as a young person with a bachelor's degree from law school at the University of Montreal, I hope that I'm going to be as brilliant as all of you when I grow up.

Some hon. members: Oh, oh!

Ms. Ève Péclet: I just want to say that I consider myself a youth and that I understand all that is going on right now with the Internet, and that I could be a victim of it. I just take it to heart the need to have the best legislation for the victims, because I've known victims of cyberbullying. I want to have the best legislation for all Canadians and for victims. That said, thank you very much and I'm going to start.

In the bill we're talking about peace officers. Peace officers not only include police services and policing but also public officers and administrators of federal acts. From questioning the witnesses from the association of police officers at the last committee meeting, it was clear that a peace officer does cover policing broadly and police services, so they don't need to include public officers and administrators of federal acts.

Why would we give extensive powers to, let's say, administrators at the Canada Revenue Agency? Does that mean that these people would have access to our information for another type of infraction?

We're talking about peace officers wanting to prosecute cyberbullies. Why include administrators of federal acts, why include public officers like mayors, etc.? Why?

My question would be for Mr. Butt and Mr. Gilhooly. Don't you think that only police officers cover peace officers broadly? Why do we need to include administrators of federal acts in Bill C-13?

● (1215)

Mr. David Butt: It's a very good question that I had not turned my mind to before you asked it. I think that based on my experience these Internet child exploitation investigations are complicated. We do a lot of training of police officers and it's important that people who are using these tools be appropriately trained.

I can't speak to what the Canada Revenue Agency does, as that's not my field of expertise. My expectation is that any law enforcement officer utilizing this should be appropriately designated and have appropriate training.

My experience is with police officers and I believe that's the core. If it extends beyond to people in other fields who don't have the training, there's a greater risk of inadvertent misuse. Then I would agree with you that it's a risk.

My experience is limited to police officers, though, so I can't comment on the extent to which those other people might have the expertise needed.

Mr. Gregory Gilhooly: Fortunately enough, the way the legislation is crafted, that too is subject to judicial oversight. There would have to be reason for the other type of administrator to be involved in the searching and uncovering of the information, the production of the information down the road.

My guess, without having drafted the legislation, is that it's there as a historical holdover from those who had similar powers before the technology came in and the technological aspect entered into the code. But again, there will be that judicial oversight, but for that provision we spoke of regarding voluntary....

Ms. Ève Péclet: Would the other witnesses like to add?

Ms. Marian K. Brown: I did turn my mind to this briefly in preparation.

As you likely know, those definitions of peace officer and public officer appear in section 2 of the Criminal Code. You have to be cautious because they apply throughout the code in hundreds of sections. When you look at the eight powers that are proposed under the lawful access provisions of Bill C-13, as I've said, seven of those are judicial authorizations. They require “informations to obtain”, these documents of dozens or hundreds of pages of justification. In reality, people who are not professional investigators are not able to meet that standard. But the one section that perhaps is amenable to use for other officials is the preservation demand, which is simply to preserve data without seizing it. That's the one provision that may be amenable to use by a broad range of officials.

Now just as a final note about the definitions, if you look at section 2 of the Criminal Code under “public official”, expecting that person to be is some kind of bureaucrat, in fact you will find that members of the RCMP fall under that part of the definition. So you have to be very careful about the effect of that definition throughout the Criminal Code.

● (1220)

The Chair: Mr. Spratt, did you have anything you wanted to add?

Mr. Michael Spratt: For once no, I think.

Voices: Oh, oh!

The Chair: Okay.

You have another minute, Madam.

Ms. Ève Péclet: Okay, great.

My colleague asked a question about the fact that these investigations would be going on and the person whose data would be provided to police officers would maybe never know about it—and there's no destruction order, too.

Maybe Mr. Spratt and Ms. Brown would like to answer my colleague's question and comment about this.

Mr. Michael Spratt: I think that's a troubling aspect. It's not just the collection of the information; it's also the retention of the information. As we've seen, with the more information you have, the more information you're able to store with modern tools. There's cross-referencing and checking, so that information can actually be mined to a large extent, which increases the potential privacy implications.

Ms. Marian K. Brown: We addressed that exact issue in our written submission. It's quite true that there isn't a specific provision for eventual destruction of copied electronic data. The older provisions of the code cover return or destruction of physical objects that are seized. But copies of data, we agree, are inadequately addressed with respect to retention and eventual destruction.

The Chair: Thank you very much for those questions and those answers.

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

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

Listening to the testimony today and from previous weeks, there seem to be three key issues that those who are concerned about the bill are raising. One is the standard, which is the reasonable grounds to suspect. I think that's an issue. Two, we're hearing about the recklessness standard is the issue. I want to focus on those quickly.

One of the things that Mr. Spratt said in his opening statement with respect to the recklessness standard for the distribution of intimate images is that it may apply to those down the chain without knowledge.

Now, Mr. Butt, you spoke about that in your statement, and I'd like you to comment on it. Would the recklessness standard apply to those who are down the chain without knowledge?

Mr. David Butt: Again, there have been hundreds of pages written by higher courts on what recklessness means, but at the risk of oversimplifying it, it's more than just carelessness. If I carelessly bump into Mr. Gilhooly, next to me, I may not even realize that he's there, but I should have realized. I'm just not even paying attention. But if I realize he's there, and I think, gee, is there risk I might bump into him, and then I go ahead anyway, that's recklessness. So people without any knowledge of the risk are not covered by recklessness, as I understand it.

Now there's another really important point here. Let's say there's a charter challenge to this legislation. The first thing the courts are going to do is to think, “We're not going to strike this down, but we're going to interpret this in way, if we can reasonably do so, that will make it survive.” What they will say is that mere carelessness goes too far. To respect the charter, they will use the more traditional definition of recklessness, which is that there has to be some knowledge of the risk, and proceeding in the face of that risk.

Mr. Kyle Seeback: So, if I were to get an e-mail chain from who knows who with an image on it, and that gets forwarded, that's not going to be someone who's reckless, right? If I have no information whatsoever as to where this image came from or the context of the image, and so I'm not going to be captured by this recklessness standard, am I?

Mr. David Butt: I don't believe you would be if there's no surrounding collateral information that puts you on notice. If it comes from a group of your friends and you happen to know that your friend just broke up with the person depicted in the image, and it comes all by itself with no.... This is an image being distributed without the person's consent—no tags on it, it just comes—but you happen to know that person just broke up with a friend of yours. I'd say you're reckless if you distribute that further, because there's something in your state of knowledge that speaks to the fact that you should be aware of that risk.

Mr. Kyle Seeback: To me, that should trigger that kind of thought process for people. I know people are young and make mistakes. I have young children. Unfortunately, they're going to be entering that Internet age with cellphones and other things soon.

They should have that thought in their mind that maybe they should do a little bit of due diligence before they redistribute that image.

I want to quickly talk about transmission data, which was the third one we discussed. My view of the transmission data is that, quite clearly, it does not include metadata. The police chiefs came and said quite clearly that it doesn't include metadata. It's very narrow and limited in scope.

I know Mr. Spratt disagrees with that, but what are your thoughts, Mr. Gilhooly and Mr. Butt, with how transmission data has been defined in this bill?

● (1225)

Mr. David Butt: I think it is wise and, indeed, necessary to stick with that narrow definition that the police chiefs have been presenting to you. I think it needs to be very clear if this comes to be interpreted by the courts that it is that narrow approach; it is not broader metadata that gives patterns.

To me, it's all about individual events that start a criminal investigation. It's not about broad intelligence about somebody's overall use. So I think that's a crucial limit and I'll defer to the experts, including the police who've been briefed by their IT people. If that's the definition they endorse, that's the one you need to have, from my perspective.

Mr. Gregory Gilhooly: And this statute is going to have to remain a living thing, because that will change over time as information and the ability to get it change. This will have to be a living and breathing document.

Mr. Kyle Seeback: Go ahead, I was going to ask you next, Ms. Brown, because in your statement you said that transmission data might reveal private conduct and—

Ms. Marian K. Brown: Yes, I was just going to speak to that.

Mr. Kyle Seeback: I hear that in a lot of submissions, that well, it may do this, it may do that. What's the hard fact behind “may reveal private conduct” in the definition of “transmission data”?

Ms. Marian K. Brown: It's a difficult point, because we accept that metadata is more revealing of private conduct, of browsing history. But transmission data, information on the mere originator and recipient of a communication, can be revealing if it's repeated. The example we gave in our written submission is of a person repeatedly contacting a specific health care provider, spending a lot of time on a mental health line, for example. That is for biographical information, and that's why we say that transmission data provisions may reveal private conduct and should be subject to the higher standard of reasonable grounds to believe.

Mr. Kyle Seeback: From my review, there are two aspects of the bill that are on reasonable suspicion, right? There's the preservation order, and I think that's largely accepted by most people as an acceptable standard. I think you recommend exigent circumstances. I think that if you're going for a preservation order, that's probably what it is, because you only get it for 21 days, and then if you want to see it you have to get a court order. But I think there's general acceptance of that.

Even Mr. Spratt, you're nodding, so I assume you generally accept that.

The issue we have is with transmission data, and it's the standard "reasonable grounds to suspect" versus "reasonable grounds to believe".

Mr. Gilhooly or Mr. Butt, why do you think the standard should be the lower threshold?

Mr. Gregory Gilhooly: I'm going to speak to this in a different context. I believe you're going to be hearing from the Canadian Centre for Child Protection later this week. I come at this concept from having been groomed in terms of the offences that were done to me.

If someone had taken a close look at what Graham James was doing to me over the first six, seven, or eight months of our relationship, there wouldn't have been anything other than, "This doesn't seem right; this is kind of out of the ordinary; something wrong is kind of, sort of, maybe going on here." So when I hear of the lower threshold, I'm immediately thrust back to my own personal circumstance. So perhaps I'm a little biased, but I'm not fussed by the lower threshold.

The Chair: Very quickly, Mr. Butt.

Mr. David Butt: In terms of reasonable suspicion for transmission data, it may or may not be totally revealing. There are a lot of examples where it will not be in an individual sense, that is, receiving one hateful bullying e-mail, for example. You need the transmission data to know who you're investigating. So because it's may or may not, that's where the other part of the bill is really important, that if the recipient of the order says you're asking for way too much, they don't have to provide it, and they can go to a judge.

● (1230)

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

From the New Democratic Party, our next questioner is Mr. Jacob.

[*Translation*]

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

Thank you to the witnesses for being here today.

My first question is for Mr. Spratt.

In your opening statement, you said you couldn't support Bill C-13 because it was too broad, wasn't constitutional and put the rights of law enforcement above privacy rights.

I'd like to hear your take on those three points. In your view, is Bill C-13 salvageable? And if so, how?

[*English*]

Mr. Michael Spratt: I think there are some important aspects in Bill C-13. Obviously, new provisions are needed to modernize the Criminal Code and to deal with some of the instances that we've heard about.

Ideally, we could split the bill and fully consider the implications of the lawful access part. But if that's not an option, what we would like to see is the appropriate standard of reasonable and probable grounds that has been endorsed by the Supreme Court in the case of Vu and corresponds with the fact that reasonable suspicion is only appropriate when the privacy level is low.

It is not enough to say that it may or may not be high, let's get the information, and if it's not high it's not revealing information—no harm, no foul. We, as lawyers, all know that there are no *ex post facto* justifications, and the fact that you find information, or that it's not intrusive after the search, can't then justify the search in the first place. That's putting the cart before the horse, and that's frowned upon by the courts.

An appropriate standard would be ideal, along with disclosure to affected persons, and legislation about the retention, use, and future dissemination of that data. Of course, tying back to some of the horrific examples of police record checks that have been in the media recently would be very valuable in this bill.

Lastly, when we're dealing with voluntary disclosure, it should be a standard that is in keeping with section 25 of the Code, a section used by the minister to justify what's already in the bill and that is one based on reasonable grounds. That means that if, as a teleco, I have something that causes me concerns, I can hand it over. But as the police, if I'm going to a telecommunications company and asking for the information, I need to show reasonable grounds, which is more than just, "We regulate you; please hand over the information."

I think those changes would be beneficial and would not set back the positive aspects and the positive intent of the first two pages of this bill.

[*Translation*]

Mr. Pierre Jacob: Thank you, Mr. Spratt.

My second question is for Ms. Brown and Ms. Schellenberg.

On page 2 of your brief, you make the following recommendation:

> The Canadian Bar Association recommends dividing Bill C-13 into two distinct bills, separating lawful access provisions from new measures to specifically address cyberbullying.

I'd like to hear your thoughts on that.

[*English*]

Ms. Marian K. Brown: That recommendation was arrived at some months ago. We appreciate that the legislative process takes its own course, but our intent in making that recommendation is simply to enable full consideration of both parts of the bill. Cyberbullying is a very sensitive topic, and lawful access is a very difficult topic both technologically and legally. Our intent in proposing a split was simply to enable a full and productive consideration of both aspects of the bill.

[*Translation*]

Mr. Pierre Jacob: Ms. Brown and Ms. Schellenberg, in your conclusion, you talk a lot about education and prevention. I'd also like to hear you comment on the importance of effective prevention and sensitive communication. Indeed, all the laws in the world won't fix all the problems in the world.

● (1235)

[*English*]

Ms. Marian K. Brown: That's for sure.

Because we are mere lawyers, we are dependent on people with expertise in education. There have been some excellent presentations from previous witnesses on how youth are being educated about the effects of cyberbullying and how they can be better educated about the effects of cyberbullying. We endorse those recommendations because, for the new offence provision to be used in a sensitive and appropriate manner, it can only go hand in hand with those educational efforts.

[*Translation*]

Mr. Pierre Jacob: Very good. Thank you.

[*English*]

Ms. Françoise Boivin: Mr. Butt, the impression you're giving me, though, is that you're relying on the courts to balance things up. What is our role? Isn't our role as parliamentarians to make sure that the bill will adopt at the end of the day, at the final stage after all readings, after hearing all the different witnesses? Is it, in our mind, the best bill that we can bring forward?

I've got a strong impression that your answers are always, "The court will do this; the court will do that; they will rebalance." When I look at the state of the courts and the access of justice, it scares me a bit for the victims actually. There's nothing more frustrating than living through a court case after all this, and giving all those tools that we all want to give, then at the end of the day the judge saying, "Do you know what? Everything you gathered under that search warrant or whatever is worth zip." That would be really sad. Maybe I'm wrong, and I didn't get you right, but that's the impression I have.

Mr. David Butt: I agree with you. That's why I say you've got the right balance. You have legislated effectively in this area, and part of legislating effectively, as my colleagues from the CBA have said, is that in seven out of eight of the new powers you've legislated judicial oversight. You have told the police that you would give them those powers, but would not give them without a leash. The leash is that, for seven out of eight, you have to go to a judge first.

Ms. Françoise Boivin: Do you find the leash is good enough?

Mr. David Butt: Yes.

The Chair: Thanks very much.

Thank you for those questions and answers.

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

Mr. David Wilks (Kootenay—Columbia, CPC): Thank you very much, Mr. Chair.

Thank you to the witnesses for being here today.

I feel a little out of place. I'm the only policeman here, and there are ten lawyers.

I want to get right to the crux of it, Mr. Spratt. You said in part of your submission that in some cases police go on fishing expeditions. I take huge exception to that. I think it's completely wrong. I don't think there's a policeman out there that intentionally says, "I think I'm going to intentionally hurt someone for the sake of hurting them and grab some information that I know will compromise case law in the future and could potentially have a ripple effect for every policeman across Canada, just because I think I can."

Mr. Michael Spratt: That happens.

Mr. David Wilks: That may be your belief; it's not mine.

Mr. Michael Spratt: The courts have found as such. I think with the definition of fishing expedition, you might be a bit wrong on that.

Mr. David Wilks: Let's just keep going because I think that using the word "fishing expedition" is a real insult to a lot of policemen who do their jobs and follow the rules very, very well every day.

● (1240)

Mr. Michael Spratt: I'm sure that a lot of police officers do.

Mr. David Wilks: From the perspective of a demand to retain information in respect to limited transmission data.... So under 162.1, as proposed, right now there's nothing there. Right now a police officer goes to a telco company and says, "Listen, we need you to hold on to something because we think there's something there, but we need you to hold on to it so that we can gather more information."

In that respect alone, do you believe this is good legislation to ensure that the police have to complete a document before a justice to ensure that they, within 21 days, come back with a warrant to get the necessary information, and/or the telco., or whatever company, says, "Have a good day. We've complied to the 21 days. We don't have to comply to this any longer."

Mr. Michael Spratt: That's a perfect example of a provision that's necessary and effective because it would allow the police to not....

Look, when we say "fishing expedition", we don't mean that the police are randomly going and seeking information.

Mr. David Wilks: Well, I think you do.

Mr. Michael Spratt: No. That's not what I mean, and that's not what the courts have said when they speak about police fishing expeditions. What we want to avoid is the police obtaining personal and private information based on their spidey senses, which happens all the time, and the courts have a dim view of that.

What provision orders allow you to do is provide the—

Mr. David Wilks: If I may interject on that for a second, as a police officer, my spidey senses, as you show them, are the one and only thing that will allow me to sometimes move forward in an investigation that will potentially bring forward more information. My spidey senses don't tell me that I can do something illegal.

Mr. Michael Spratt: Well, unfortunately, spidey senses don't amount to reasonable and probable grounds, and the courts have found that acting on spidey senses or mere suspicion is what leads to evidence being excluded.

When police act on their spidey senses and don't have the requisite reasonable and probable grounds to do an act and yet they do it anyway, I respectfully disagree. In that case, the police have acted illegally.

Mr. David Wilks: Would you agree that if a police officer has reasonable and probable grounds and applies for a warrant, through the Criminal Code or any other act of Parliament, that it has had judicial review?

Mr. Michael Spratt: Yes. That's what I'm imploring you to do in this bill, to change that and add that.

Mr. David Wilks: That's what we do in all of it, with the exception of the demand order. It's reasonable and probable grounds. All of those things with regard to the wiretap are still there. In fact, we still have to notify within 60 days.

I think it's too short, personally. I think it should be longer. I can tell you from personal information that I lost a case in the Supreme Court of British Columbia in which we were not able to notify within 60 days everyone who was wiretapped. I think it was a miscarriage of justice when that happened, but unfortunately that's the law as it is right now.

To say that people are not notified is utterly wrong; they are notified within 60 days.

Mr. Michael Spratt: Show me the notification in this bill. It's not there.

Mr. David Wilks: I'm telling you that it is there.

That's fine. You don't have to agree with me, but I'm telling you from a police perspective that this bill does a lot more than what we have now.

Mr. Michael Spratt: You know that notification under wiretap provisions and the sections in here are completely different; there is no notification provision in here.

Mr. David Wilks: I'll show it to you afterwards.

My other question would be for the Canadian Bar Association. With regard to the preservation demand under this act, do you believe—as I've asked Mr. Spratt—that it furthers the protection of both the victim and the police in doing their job?

Ms. Marian K. Brown: Yes, but we have proposed a number of refinements, the first being that it should be used only in exigent circumstances. We accept that when data is to be deleted, automatically or otherwise, that it may be in exigent circumstances.

Mr. David Wilks: Could you give a definition of exigent circumstances?

Ms. Marian K. Brown: In this context, we've made a specific recommendation that it would be in circumstances where the data would otherwise be deleted in the time required to obtain a judicial authorization.

Mr. David Wilks: Could you give me an example of how the police would know that the data is going to be deleted? How would they know it without their spidey senses?

Voices: Oh, oh!

Ms. Marian K. Brown: Well, they're making a demand of a particular service provider or website that may have automatic deletion of data, so there may be a known time parameter, or there may be a suspicion that the perpetrator will delete it. I don't think that reasonable suspicion is the same as spidey sense, but reasonable suspicion is, in our view, an appropriate level for this type of provision.

But we distinguish between provisions of this bill that appropriately use the reasonable suspicion standard and provisions that will be subject to charter challenge unless they use the "reasonable grounds to believe" standard.

● (1245)

The Chair: Thank you very much for those questions and answers.

I do ask both the members of the committee and the witnesses to be respectful of each other in the use of language. Thank you very much.

The next questioner is Madam Boivin from the New Democratic Party.

Ms. Françoise Boivin: I have a quick question for you, Mr. Spratt. Would it be possible to obtain your views on key recommendations of amendments—

Mr. Michael Spratt: Of course.

Ms. Françoise Boivin: —and where you think we should specifically make changes, and the wording? We just love it when people do our jobs for us, in a sense. It helps just to be accurate.

I don't necessarily want you to state them right now. You can do it later and provide it to the committee, and we would be very appreciative. If you have them all, well, we'll give you the time to say it.

The Chair: We'd appreciate it if you sent it to the clerk so that all members could have it and it would be translated.

Ms. Françoise Boivin: Yes, exactly, and it would be translated. That would be awesome.

Meanwhile, I'll address the Association du Barreau canadien, because I really appreciate the work you've done in trying to look at all the parts of the bill.

[*Translation*]

The Canadian Bar Association has done some wonderful work here. That said, there are some recommendations I'd like to understand a bit better, including the fifth one, which reads as follows:

> The Canadian Bar Association recommends adding to section 162.1: No person who is a provider of telecommunications services, information location tools, or network services shall be convicted of an offence under this section unless that person solicits, counsels, incites or invites another person to commit an offence under this section, regardless of whether or not that other person commits the offence.

Why did you make that recommendation?

[*English*]

Ms. Marian K. Brown: This recommendation was made after input from our privacy law section regarding the role of online service providers such as search engines and social media websites, which may not have any monitoring of material that is posted or retrieved through their services. So where there is no knowledge, no *mens rea* on the issue of consent, of whether dissemination of an image was consensual or not, there should be no criminal liability.

However, there are websites that exist for the purpose of revenge porn or other non-consensual dissemination of images. Those websites would likely meet one of the bases of culpability, those being solicits, counsels, incites, or invites—probably invites—and would thus be parties to the offence.

Ms. Françoise Boivin: So just to be clear, because I remember one of the witnesses—and I don't remember her name—saying that she had a horrible, horrible page that was, let's say, put on a certain social media.... She approached the social media site, which said that it didn't breach any of their whatevers. How do you classify that in virtue of your fifth recommendation?

Ms. Marian K. Brown: It's probably still not culpable—

Ms. Françoise Boivin: I was afraid you'd say that.

Ms. Marian K. Brown: —according to the wording that we've provided. Criminal *mens rea* is a high standard.

Ms. Françoise Boivin: I know.

Ms. Marian K. Brown: The intent to commit a criminal offence is a high standard. The wording of the offence section is not going to solve all the problems that exist with the Internet.

Ms. Françoise Boivin: So I'll just suggest that we make them a helper in the whole situation.

Ms. Marian K. Brown: Good luck with that.

Ms. Françoise Boivin: Okay, thank you. That was that for that one.

Number 8, I thought was interesting. It reads:

[*Translation*]

> The Canadian Bar Association recommends creation of a single entity to consider the nation-wide impact of the seizure, retention, and use of personal information by Canadian law enforcement agencies.

Could you elaborate a bit on what exactly you mean by that?

● (1250)

[*English*]

Ms. Marian K. Brown: Yes. It addresses seizure but also retention of personal information. That falls under the privacy acts of all the provinces, as well as the federal Privacy Act. All police agencies are public bodies that are subject to those privacy acts. So we don't see that it could be anything other than a nationwide and interjurisdictional effort to address the impact of retention and use of personal information by law enforcement agencies.

We're pushing the envelope here but the point is, as I said in my introduction, that as good as you make Bill C-13, it is not going to solve all of the concerns that we face in this confrontation of law and technology.

Ms. Françoise Boivin: In recommendation 11 you say:

[*Translation*]

> The Canadian Bar Association recommends that if officers are granted power to make preservation demands, written records should be required to set out the bases upon which demands were made.

How long would those written records be kept for? Who would have access to them? Those are the questions that come to mind.

[*English*]

Ms. Marian K. Brown: I think that someone who has worked in law enforcement directly could answer that question better. But my understanding is that retention periods for law enforcement files are very long, up to 99 years.

The purpose of this provision is so that there is a justification of this warrantless demand. All of the warrants and production orders, as I've said, have a record of justification in the information to obtain that is filed in the court registry. The preservation demand is the only one of these eight powers for which there is no reporting mechanism. The same issue has been encountered under part VI, the wiretap part of the Criminal Code, with the interceptions in exceptional circumstances that were addressed in the Tse case. One of the shortcomings was the lack of reporting, and that was remedied by an amendment. So I think that is an obvious amendment for this provision.

Ms. Françoise Boivin: Thanks.

The Chair: That's it for questions and answers.

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

But before I go to him I just want to let the committee know that we normally meet here at La Promenade building, but on Thursday of this week we are meeting at Queen Street. So that's just a heads up for you to remember.

Mr. Dechert, the floor is yours for the next few minutes.

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

Ms. Brown, I want to come back to a couple of comments you made about the recommendations of the Canadian Bar Association.

In response to a question from Mr. Jacob you mentioned that one of the recommendations of the Canadian Bar Association was to split the bill into two parts. That was put forward some time ago on the theory that the bill needed full consideration of all parts; it was to enable full consideration of all parts, you said.

Have you reviewed the witnesses that appeared to date?

Ms. Marian K. Brown: I have.

Mr. Bob Dechert: You may or may not know who will be appearing before the committee in the next two weeks, but I can let you know that there will be at least two more weeks of hearings on this. There have been several days of debate in the House of Commons and there'll be several days more when we get to third reading. How much more study and debate do you think is required?

Ms. Marian K. Brown: I'm not prepared to comment on the parliamentary process. My concern however was that there be—

Mr. Bob Dechert: Can I just mention one other thing because I think it's important for you to know this. Virtually every witness submitted by every party has or will be heard from. So what are we leaving out?

Ms. Marian K. Brown: I think what's been missing from the process, and there may not be a remedy in the parliamentary process, is public understanding of what this bill is about. We all know how polarized the debate is. It's very unfortunate that important witnesses such as Carol Todd come to this venue and say that they don't understand parts of the bill.

Mr. Bob Dechert: I understand that.

Ms. Marian K. Brown: So that was our concern.

Mr. Bob Dechert: So Mrs. Todd met with the Minister of Justice following her appearance here. Then she did an interview on CBC Radio a week ago Friday, the Friday before the long weekend, which I had an opportunity to hear. I don't know if you've seen a transcript of it where she changed quite substantially her views on the bill.

Did you hear that interview?

Ms. Marian K. Brown: I heard it and I reviewed her transcript. I don't think she was substantially inconsistent. But as I said, I'm not taking any position on the process. We only want there to be—

● (1255)

Mr. Bob Dechert: So it's time.

Ms. Marian K. Brown: — the best possible debate on this.

Mr. Bob Dechert: How much time do you think is necessary?

Ms. Marian K. Brown: I'm not proposing any particular period of time.

Mr. Bob Dechert: You've talked a lot about preservation of evidence in exigent circumstances, which I take you to be mean situations where the evidence is likely to be destroyed.

Ms. Marian K. Brown: Yes.

Mr. Bob Dechert: Help me out here. Why would the preservation of evidence of a potential crime ever be a bad thing?

Ms. Marian K. Brown: Oh, I'm not suggesting that it is. But it still has to meet a standard for the demand, which is proposed to be reasonable suspicion, and we agree that standard is a—

Mr. Bob Dechert: It's not disclosure, though, of the evidence, correct? It's just preservation.

Ms. Marian K. Brown: Yes, for preservation.

Mr. Bob Dechert: So is there a circumstance where there might have been a crime committed where the Canadian Bar Association would be prepared to see that evidence destroyed because it didn't meet a particular standard?

Ms. Marian K. Brown: If you're speaking of evidence that remains in private hands, which is what we have here—

Mr. Bob Dechert: So we're just asking an ISP provider, for example, to hold on to the information until a judge can make a preservation ruling.

The Chair: We have a point of order from Mr. MacAulay.

Hon. Lawrence MacAulay: It's a point of clarification.

The Chair: That's not a point of order.

Hon. Lawrence MacAulay: On a point of order, I just need to understand this. I would like to ask Mr. Gilhooly, if there's no judicial oversight, is that—

The Chair: That's not a point of order. Nice try, though.

Mr. Dechert, the time is yours.

Thank you for showing up for this meeting. We look forward to your not coming back again.

Voices: Oh, oh!

The Chair: Thank you, Mr. MacAulay.

Mr. Dechert.

Mr. Bob Dechert: All right. Where would the Canadian Bar Association come down on it's a good thing to destroy the evidence versus preserve it if it could provide evidence of a crime that needs to be investigated and prosecuted?

Ms. Marian K. Brown: We're not taking a position on whether a private individual makes the choice of retaining or deleting data. What we take positions on is the authority of law enforcement to control that data in a sense of requiring that it be preserved. The standard of reasonable suspicion appears appropriate to us for obtaining a preservation demand.

Mr. Bob Dechert: So you think that there's a situation where it would be okay to let the evidence be destroyed. I'm trying to understand this in layman's terms. Help me out. I'm not a criminal lawyer here. I can't imagine why you would want to allow somebody to destroy evidence of a crime if it would help to prosecute and bring the person responsible for that crime to justice. I don't understand.

Ms. Marian K. Brown: I'm not sure that I understand your question.

Mr. Bob Dechert: I'm having trouble understanding the Canadian Bar Association position here.

The Chair: Okay, one speaker.

One minute.

Mr. Bob Dechert: Okay, Mr. Gilhooly, you mentioned that you were a corporate counsel. I've done that as well. If your client received a request from the police to turn over information and they came to you and said, “Can we, or should we disclose this”, does the immunity provision help you in advising your client?

Mr. Gregory Gilhooly: Absolutely. Absent the immunity, my first answer is going to be no, because the easy lawyer answer is no. Show me your warrant. Absent a warrant, I don't have to do it. I'm not doing it. It makes it very difficult for me to do the right thing. That's the issue that you were raising I think in one of the hypotheticals with David Fraser earlier.

The Chair: Thank you very much.

Thank you panel for coming. We've had some very good panels for Bill C-13 and today's testimony was excellent. I want to thank each and every one of you.

Just as a reminder, we're meeting on Thursday morning at Queen Street. We have Thursday and then next week to meet on this, and then we'll do clause by clause the week after that.

Thank you very much.

The meeting is adjourned.