HOUSE OF COMMONS
CHAMBRE DES COMMUNES
CANADA

Standing Committee on Justice and Human Rights

JUST • NUMBER 022 • 2nd SESSION • 41st PARLIAMENT

EVIDENCE

Tuesday, May 6, 2014

Chair

Mr. Mike Wallace

Standing Committee on Justice and Human Rights

Tuesday, May 6, 2014

● (1100)

[*English*]

The Chair (Mr. Mike Wallace (Burlington, CPC)): Ladies and gentlemen, I'm going to call this meeting to order. It's meeting number 22 of the Standing Committee on Justice and Human Rights.

As per the orders of the day and the orders of reference of Monday, April 28, 2014, we are dealing today with Bill C-13, An Act to amend the Criminal Code, the Canada Evidence Act, the Competition Act and the Mutual Legal Assistance in Criminal Matters Act.

We have three groups of witnesses here today. Here as an individual, we have Mr. David Fraser, who is partner in the law firm of McInnes Cooper. From the Boys and Girls Club, we have with us Marlene Deboisbriand, the vice-president of member services, and Fahd....

What's your last name, Fahd?

Mr. Fahd Alhattab (Alumnus, Boys and Girls Clubs of Canada): It's Alhattab.

The Chair: Fahd Alhattab is here with the Boys and Girls Club.

I want to thank Steph Guthrie for joining us by video conference.

Where are you from, Ms. Guthrie?

Ms. Steph Guthrie (Feminist Advocate, As an Individual): I'm hailing from Toronto today.

Hello. Thank you for having me.

The Chair: It's nice to see that the audio system is working.

We'll give each witness group about 10 minutes for their opening statement. Then we'll go around the table with questions for the next couple of hours.

With that, the floor is yours, Mr. Fraser.

Mr. David Fraser (Partner, McInnes Cooper, As an Individual): Thank you very much.

Thank you very much for providing me with the opportunity to speak with you and the committee today.

For the purposes of introduction, my name is David Fraser. I'm a partner with the Atlantic Canadian law firm McInnes Cooper, but I do need to emphasize that I'm here speaking as an individual. My comments and opinions shouldn't be attributed to my firm or its clients or other organizations with which I'm associated.

I've been practising Internet and privacy law for over a dozen years now. I've represented a range of clients over the years, including victims of cyberbullying, victims whose intimate images have been posted online, and I have represented and advised service providers.

Most notably, I was part of a team at my firm that took the case of a 15-year-old girl, a victim of cyberbullying, to the Supreme Court of Canada. This was the first time that the court had the opportunity to consider the phenomenon of cyberbullying, and the unanimous court came out very strongly to protect the interests of this victim of sexualized cyberbullying. But I've also advised people who have been accused of cyberbullying, and I hope that this experience from a number of different perspectives will provide this committee with some assistance in its very important task of considering Bill C-13.

First, looking at the bill as a whole, I'm disappointed that Bill C-13 combines two very different but related matters: the dissemination of intimate images on one hand, and law enforcement powers more generally on the other hand. Both aspects raise very important issues that merit close scrutiny, but we're seeing the debate about police powers as overshadowing the discussion about cyberbullying. That said, we do have one bill in front of us and I'm pleased to provide you with my thoughts.

It has been suggested that Bill C-13, if it had been enforced, could have saved Amanda Todd and Rehtaeh Parsons and other young people. That makes a good sound bite, but the world is much more complicated than that. The creation, possession, and dissemination of child pornography is and was a crime. So is the creation, possession, and dissemination of voyeurism images. So is extortion. So is criminal harassment. So is sexual assault. But that said, there is a gap that we should fill, which is the malicious dissemination of intimate images without the consent of the person depicted in them, regardless of the age of the person depicted in the image.

We need to be very careful about how we craft this offence, however. The current reality is that young people and adults, whether we like it not, take photos of themselves and voluntarily share them with intimate partners. Those digital images can easily be spread around without the consent of the person depicted. We want to criminalize the boyfriend who posts pictures of his ex-girlfriend online without her consent, the so-called revenge porn. We want to criminalize the actions of the person who forwards around images of current or former intimate partners. In each of those cases, the individual would know, or ought to have known, whether they had the consent of the person depicted in those images.

But we need to be cautious. We shouldn't inadvertently criminalize behaviour that's not blameworthy. Someone finds a picture online of someone naked—I understand there are pictures of naked people on the Internet—and forwards it to a friend. That person knows nothing about the circumstances in which the photo was taken. It could be a professional model. The photo could have been posted by the person in the photo herself. There's no way to tell whether consent was obtained, whether there was any expectation of privacy at the time that the image was created, and the individual, in this case the accused, would have no way of determining this, would have no way of contacting the person in the image to find out. So the real challenge arises when addressing third parties who do not know the person depicted in the image, nor do they have knowledge of those circumstances in order to figure it out.

The provisions in the bill use a recklessness standard, which in my view is too low. Recklessness applies where a person should have looked into it but decided to be wilfully blind. However, given the huge number of images online, it's not possible to look into it. This is especially important for online service providers, who have no way of knowing and no way of finding out the circumstances under which an image was taken or uploaded. We need to be especially attentive to crafting the law so that it will survive a challenge in the courts, and recklessness poses a risk of having a law struck down or making criminals out of people who are not truly blameworthy.

Turning now to the part of the bill related to police powers, the first one that I'd like to speak about is transmission data. Bill C-13 creates a production order for transmission data and warrants for transmission data recorders. It has been said that the purpose of the transmission data provisions of the bill is to extend the current police powers—which are coupled with judicial oversight, I'm very pleased to see—related to telephone information and move that over to the Internet age, the idea being without significantly altering the status quo, simply altering or modernizing what's already an existing police power.

While this may be a very reasonable objective, this must be done also very carefully, because transmission data in the Internet age is very different from transmission data in the traditional plain old telephone system. With conventional telephony, transmission data refers to the number called from, the number called to, whether the call was connected, and how long that call lasted.

● (1105)

In the Internet context, the amount of information that's included in the kind of out-of-band signalling information and what it reveals is dramatically different. It would include the IP address of the originating computer, the destination computer, information about the browser that's being used, information about the computer that's being used, information about the URL, the address being accessed, which can actually disclose content, even though the definition of transmission data is intended to exclude that.

It will also tell you what kind of communications are being done. Is it an e-mail communication? Is it an instant message? Is it peer-to-peer file sharing or otherwise? So it provides much more insight into actually what is going on than just phone number information.

An interception of transmission data would tell law enforcement agencies whether the target of surveillance was visiting a search engine, an encyclopedia site, a poker site, or a medical site. Furthermore, the data would provide greater insight into the likely physical location of the surveillance target. This is a dramatic expansion of the information that's provided and available, compared to traditional telephone communications.

As anybody in this room knows, I expect, the way we use computers today is dramatically different from the way we used telephones 15 years ago. We use them as spellcheckers. We use them to find out facts. We use them for a much wider range of activities. With the disclosure of greater information through these transmission data orders, you're revealing much more about an individual. Even though the definition excludes content, just the transmission data tells you a lot more about really what's going on.

I would suggest this can be fixed by either raising the standard from reasonable grounds to suspect to reasonable grounds to believe with respect to this data, or re-crafting the definition of transmission data, so we're sure that we are, in fact, paralleling what is intended, which is to take the telephony tool and move that into the modern Internet age.

I would also note that in all of these orders—again, I'm pleased that they're subject to judicial oversight and judicial approval—there is no mechanism in these for notifying the individual after the fact that their information has been accessed, which I think is something that happens with respect to wiretap orders. Certainly it happens with respect to search warrants. I believe that should be extended into this environment as well for these sorts of production orders.

Finally, I would touch very briefly on the issue of service provider immunity that's touched on within this statute. I find this to be gravely problematic. I think it's a very cleverly crafted provision. We're told that this is simply for greater certainty, but it goes beyond that. Everything we know suggests otherwise.

It says that you will not be liable for handing over any data that you're not prohibited by law from handing over, and if you do so you're civilly immune. Now, only the criminal law and other regulations create prohibitions against handing over information, but you can hand over information when you're not legally prohibited and still incur civil liability. Civil liability is there for a reason. I may not be legally prohibited from accidentally driving my car into yours, but if I do that, you're entitled to damages from that. I should be paying for the harm that is caused.

If there were an immunity provision that said you could not sue me if I did something that was not legally prohibited, that would be squelched. That would go away. So this provision, I believe, should be removed. It can't be fixed and will only encourage overreaching by law enforcement.

In conclusion, while we don't have Bill S-4, the digital privacy act, in front of us, that fits together with the immunity provisions. I'm concerned that the two taken together will extend the amount of information not only available to law enforcement but will extend the information available to other civil litigants and others. Although I understand it's not within the jurisdiction of this committee, I flag the fact that Bill C-13 and Bill S-4 do, in fact, fit together, and somebody should look at that interrelationship.

Thank you very much for this opportunity to speak with you today. The cyberbullying provisions are an important step forward and will, if properly tweaked, address this very serious problem. The rest of the bill needs to be very closely examined to ensure that it does what it is supposed to do and nothing more. It should be about providing the police with appropriate tools, with adequate thresholds and accountability, and judicial oversight, but not redrawing the line with respect to personal privacy.

I very much look forward to discussing this issue with you further. Thank you.

● (1110)

The Chair: Thank you, Mr. Fraser. Thank you for those comments. There will be questions, I'm sure, afterwards.

Next we will go to the Boys and Girls Clubs of Canada and Madam Deboisbriand.

The floor is yours. You can share your time however you wish.

Mrs. Marlene Deboisbriand (Vice-President, Member Services, Boys and Girls Clubs of Canada): I'm going to hand my time over to Fahd, who is a youth from one of our clubs.

The Chair: The time is yours. You have 10 minutes.

Mr. Fahd Alhattab: Fantastic. Thanks for having me, guys.

I'll give you some quick background about myself. My name is Fahd. I'm an Ottawa native. I've been here for about 16 years now. I like to say that I grew up at the Boys and Girls Club. I've been going there for about 10 years as a kid, and I started volunteering. Today I work there as both a volunteer and as a staff member. Thank you for having me here today at committee to speak about Bill C-13, the protecting Canadians from online crime act.

As some of you might know, the Boys and Girls Clubs of Canada are leading providers of quality programs for the healthy development of children and youth. Our association has 99 clubs and reaches over 200,000 children and their families in over 650 community service locations across Canada. So we're vast, and we really work with a lot of youth and really understand the issues that they're facing and the issues that we need to address.

Let me start off by saying that we very much welcome the action to address the harms of cyberbullying. We're concerned about the far-reaching consequences of cyberbullying and think that Bill C-13 is proposing to address one of the harmful manifestations of cyberbullying and the non-consensual sharing of intimate images.

Currently, young people who share intimate images of minors, and sometimes their own peers, are being charged with child pornography. We think this legislation is obviously more appropriate as a response than the use of criminal pornography charges. In this sense, we say thank you. This is a very positive step that Bill C-13 is taking forward.

We understand that Bill C-13 has also raised concerns on the respect of privacy. Young people deserve to be protected from cyberbullying, but they also deserve to be protected and respected for their privacy. Now, we're no experts on privacy, so our only recommendation on that is to encourage you to listen, obviously, to any concerns that are brought up, any considerations that are brought up, by the experts who are dealing with privacy, to make sure that we're protecting youth from cyberbullying but we're also protecting our children and youth and their privacy rights.

I have three main points that I'm going to bring up. Hopefully you can follow my train of thought; sometimes I ramble.

First, I want to talk about the importance of consulting with some of the youth that we work with. Bringing in legislation is great, but sometimes we have a different view on how the world of the Internet works for us and how it works for them. Second, to coordinate efforts across Canada, I'll be talking a bit more about the different legislation that's happening in different provinces. Unfortunately, the Internet doesn't really have borders. We have to take that into consideration. We also have to look at restorative justice versus criminal punishments.

I'll start with the first point, the consultation with youth. Young people are more connected. You all know this, and those of you who have kids. Young people are more connected that any generation before them. A recent study conducted by MediaSmarts actually polled 5,000 youth from grades 4 to 11 in the provinces and territories and found that youth in Canada have a universal access to the Internet: 99% of them have access to the Internet outside of school. We're digital natives. Twenty-four percent of grade four students have their own cellphones and that percentage increases to 85% by grade 11. The reality is they have access to everything and they're using it to socialize with peers. They're using it to find information. They're using it for sports, sexuality, and health. They're testing their boundaries, right? It's natural. It's a natural fit. So with the increased connectivity and the new social norms around electronic communications, young people are vulnerable to cyber-bullying.

As David said, a lot of young people are victims of cyberbullying, and this bill will affect them the most. So my recommendation is that it is very important to speak to the youth and really understand where they're coming from and how they see that it will affect them on a very detailed basis.

● (1115)

To the second one, the desire to address cyberbullying has resulted in a patchwork of legislation across Canada. That really creates risks for children and youth confused about their responsibilities and rights, and the legal repercussions of their actions.

The Standing Senate Committee on Human Rights and the CCSO cybercrime working group both recommended that the federal government play a lead role in coordinating efforts to address cyberbullying, in part through a national prevention strategy, legal education, and digital citizenship. Whatever is decided and happens and moves forward, we argue that the leaders need to take charge, coordinate the message, and make sure that the federal government is playing a very strong role.

The government's new campaign, Stop Hating Online, is fantastic. That's great. Those are the kinds of things we need. Taking the time to partner with organizations like the Boys and Girls Clubs of Canada, which serves 200,000 youth, would be even a bigger step, the next step forward. These campaigns are important. They really help what we're trying to do by educating young people and really moving them forward.

The last one is around restorative justice. We like to think we can educate our youth, but despite our best efforts the kids will break the rules. We were all kids. We work with them, or we have kids—I don't have any yet—but the reality is that's what's going to happen. You can imagine that to punish a sixth grade kid for pressing "send" on a cellphone and sending a picture that he received to a friend.... Giving him a legal punishment of child pornography doesn't seem logical to me. I know that many of you will agree with that.

What we've done is we have restorative justice programs. These foster responsibility in the wrongdoer and ensure accountability and meaningful consequences for the crime. The impulsive sharing of intimate images without consent, with no severe malicious intent, is perfectly suited for this type of intervention.

The Boys and Girls Clubs in British Columbia, Alberta, Yukon, and Ontario have been offering youth restorative justice programs for several years now with great success. In recent years we've actually been referred sexting cases.

The Ontario Provincial Police recently reached out to the Boys and Girls Clubs of Kawartha Lakes, to ask if they would partner with them to respond when youth are accused of sexting. The OPP will refer cases of youth between the ages of 12 to 17. The clubs' restorative justice program has been well established and has a very solid track record.

Similarly, Durham Regional Police Service refers sexting cases to the Boys and Girls Clubs in their area as part of the pre-charge program. The club has seen a few of these cases now, and prepares individual restorative plans for each case, because each case is different for many of the youth in how it ends up unfolding.

Obviously, as we know, education around this plays a big role, and it has involved educating minors about the consequences of sharing these intimate images and how sharing puts the recipient at risk of child pornography charges. As they come to understand this, their actions change and they understand the legal repercussions behind sharing these images.

As I said, a lot of our programs are very refined for the youth and very tailored to the youth, customized to them. The measurement sanctions are dependent on the severity of the offence. A lot of times we see young people who don't have the malicious intent but kind of go with it, and they end up having charges that are not adequate for them.

To summarize, let's protect the privacy of our children at the same time as we protect them from cyberbullying.

Let's consult with youth about the importance of this bill and how it affects them, and how we can ensure it protects them.

Let's coordinate our efforts across Canada to make sure that everyone is receiving the same understanding, and understand that the Internet does not have borders.

Let's take a restorative justice approach instead of a criminal offence approach.

Thank you.

● (1120)

The Chair: Thank you, sir.

Very good. Thank you for those comments. There will be questions in the next round.

Our final speaker for today is Ms. Guthrie, from Toronto, on video conference.

The floor is yours.

Ms. Steph Guthrie: Thank you for having me here today.

I'd like to thank my fellow witnesses, who both had really eloquent and valuable things to say.

My name is Steph Guthrie. I am a freelance feminist and digital strategist. For the last year I have been speaking and writing at length about the issue that Bill C-13 claims to tackle.

While the bill's name in the press is the "cyberbullying" bill, the more specific problem that I think is addressed by components of Bill C-13 is actually known as "revenge porn" more specifically, a term that I hate for both its inaccuracy and its sexualized sensationalism. Whatever you call it, though, we're talking about sharing sexually explicit images without the consent of the person or persons depicted. While some such cases might involve hacking, in many cases the subject actually consented to share the images with one person for private use, such as a sexual partner, and that person then violates their trust and shares the image with others, despite the subject's in most cases obviously implied expectation of discretion.

The crux of the harm that is inflicted here is the violation of informed consent. If I share an image with another person privately, that consent is not transferable. Had I known that the other person might later share the image with others, I would be unlikely to consent to letting that person access the image in the first place. So any consent I provide to a person accessing that image is pretty clearly contingent on them keeping it to themselves.

For me, informed consent is an integral part of privacy. Indeed, in her influential privacy by design framework, Ontario Privacy Commissioner Ann Cavoukian cites freely given and specific consent as a vital element of digital privacy. Cavoukian's principle can be applied to non-consensual intimate image sharing, which—let's be honest—is a really clunky and cumbersome way of describing what is ultimately cybersexual assault. A survivor of cybersexual assault did not provide specific consent for their image to be shared with others. The perpetrator simply treated their consent as transferable to any other use, any other disclosure.

As I'm sure some other speakers over the course of considering this bill will share with you, the results of this are devastating. It does mostly happen to women, although men are not immune, and it destroys their lives. The images follow them into their job interviews, on their first dates, and to the laundromat. In some cases the perpetrator of the cybersexual assault incites violence or stalking against the survivor, publishing their personal information and the dates and times of their professional engagements, encouraging their "fans" to make an appearance.

In any case, the assault constricts the survivor's ability to live life normally and comfortably because they are constantly living with the idea that the people they encounter in their day-to-day lives may know intimate things about them that they didn't consent to share. Even if the survivor knows they did nothing wrong, they still must deal with the judgments, misperceptions, and intrusions of others. For many survivors, their ability to move freely, safely, and happily in this world is limited.

I am fortunate to not yet have been attacked and tormented in this way, but I could be. It's common for authorities and the media to malign people who send so-called sexts as teenagers with poor judgment and poor impulse control. But that doesn't line up with reality. According to a Harris Poll in 2012, a full 40%—that's not a majority, but it was the largest percentage—of people who send these images are in the 18 to 34 age range; and 20% of all adults sext. In fact, a McAfee survey puts that number closer to 50%. I'm willing to bet that a lot more than 50% of us have trusted a romantic or sexual partner only to learn later that our trust was misplaced.

Cybersexual assaults can and do happen to a lot of us. When Rehtaeh Parsons died by suicide after months and months of torment from her peers and indifference from authorities following her own sexual assault, first in the flesh, then online, I heard Prime Minister Stephen Harper say: "...we've got to stop using just the term bullying to describe some of these things....What we are dealing with in some of these circumstances is simply criminal activity."

While I join my fellow witness in favouring a restorative justice approach, at the time I was already a vocal advocate for legislation to tackle cybersexual assault, and was accustomed to hearing political and legal decision-makers blame the victim for it. So I was cautiously optimistic at Prime Minister Harper's remarks.

● (1125)

Then I realized, as many Canadians realized, that most of Bill C-13 is not really about what happened to Rehtaeh Parsons. Buried within Bill C-13 is a set of decent Criminal Code amendments to tackle cybersexual assault. Though I do see some minor issues with those amendments, which my fellow witnesses have already covered off quite well, and I can certainly refer to them in greater length during the Q and A, I do think that the base for good cybersexual assault legislation is there in Bill C-13. But you have to dig pretty hard to find it amid the many other sweeping amendments that more closely resemble the lawful access provisions found in Bill C-30 back in 2012. That was the time when Canadians were told that opposition to the bill was tantamount to supporting child pornographers.

While some of the more egregious elements of the former Bill C-30 have been removed from this latest incarnation—and I'm glad to see that—it still significantly expands the state's capacity for surveilling Canadians without the pesky oversight of our court system.

One of the most troubling provisions in Bill C-30 was that it mandated the disclosure of user information to police without a search warrant. The newly designed provision in Bill C-13 very cleverly softens this, instead stating that police can request information, and the person or organization to whom they direct their request can voluntarily comply. However, the very next provision in Bill C-13 removes all civil liability for anyone who discloses another person's information to police upon request. This granting of immunity removes much of the incentive for an Internet service provider, or anyone else, to deny the request.

As law enforcement officers and prominent figures of power and authority in our lives, it is also debatable the extent to which a person might feel compelled to provide the information to a police officer, even if technically they are volunteering to do so.

In the last week, a steady stream of damning media reports have indicated that the practice of voluntarily disclosing user information to police is already in full swing among Canadian telecommunications companies, with the state making over a million requests for user information in the course of a year—and that was back in 2011—all without warrants, i.e., without due process. All were quite obviously without users' consent.

Perhaps most of Bill C-13 isn't really about cybersexual assault, but I find it interesting that it violates some of the same privacy principles, such as freely given and specific consent. Most of us do not and would not give free and specific consent for the state to access any, and potentially all, of our data by way of our Internet service providers if we had any meaningful choice in the matter.

The consent we give is to our Internet service providers. If the police want our information because they suspect we are engaged in criminal activity, well, most of us would assume that is what search warrants are for.

Bill C-13 enshrines the idea of transferable consent in law, immunizing anyone who shares our information and violates our privacy without adequate legal justification for doing so.

While obviously different in many ways, the limitations on personal freedom imposed by Bill C-13 bear some striking similarities to those imposed by cybersexual assault. The state could be following us into our job interviews, on our first dates, or to the laundromat. The bill's provisions will restrict Canadians' ability to live life normally and comfortably because they are constantly living with the idea that the state, when they encounter it, may know intimate things about them that they didn't consent to share. Even if they know they have done nothing wrong, they must still deal with the judgments, misperceptions, and intrusions of the state.

For many Canadians, if Bill C-13 passes as written, our ability to move freely, safely, and happily in this world will be limited. That's why it pains me to say that after a year of arguing for legislation that criminalizes cybersexual assault, I cannot support this legislation as written. We should separate the components of Bill C-13 that deal directly with cybersexual assault from those that do not and debate them as different pieces of legislation. They are different issues.

Not only would this be in the best interest of Canadians, but I believe it would do greater justice to survivors of cybersexual assault than amalgamating their cause with another one that serves the state's pursuit of power more than it serves Canadians.

Thank you.

● (1130)

The Chair: Thank you, Ms. Guthrie, for those comments.

We are going now to the question and answer period.

Colleagues, because we have a video conference, it would be helpful if you let us know who your question is directed to or whether you want everyone to respond.

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

[*Translation*]

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

My thanks to all the witnesses here for coming to help us hopefully improve Bill C-13.

But I would like to tell Mr. Fraser and Ms. Guthrie from the outset that we share your opinion that it would have been preferable to divide the bill. The representatives from the Boys and Girls Clubs of Canada are saying the same thing. We introduced a motion in the House to divide the bill, listing exactly the same sections that the Boys and Girls Clubs of Canada mentioned in their brief. Unfortunately, we were not successful.

Everyone has their own expertise and there are people who have extremely specialized expertise in privacy, in electronic surveillance, in all kinds of areas. Unfortunately, we have to get down to the task and look at all the provisions.

[*English*]

I do not want to rain on your parade, but we tried and the government said no. That being said,

[*Translation*]

you raised some quite interesting points in connection with some of my concerns. I might like us to talk about them in a little more depth.

I do not want to ignore what the representatives of the Boys and Girls Clubs of Canada said. I heard their message. We had a meeting about it too. Actually, that was where the idea of dividing the bill came up. Most people do not see a lot of problems in the first part, but they see huge ones in the second part.

Mr. Fraser, you talked about the burden of proof. The burden of proof, to me, is the difference between reasonable grounds to suspect and reasonable and probable grounds to believe. Those terms are a little more familiar for those who have practiced criminal law.

For the benefit of the committee, could you highlight the distinction between the two? I do not know if you have read the minister's response. He seems to feel that a burden of proof based on reasonable and probable grounds to suspect is already well accepted by the courts.

I will ask you the same question, Ms. Guthrie.

Mr. Fraser, could you also spell out for me your position on immunity. I am not sure I completely grasped it.

Section 487.0195(1) says as long as it is “not prohibited by law ”. What specifically does that refer to? Does it affect the Charter? If I have the right to privacy, does the fact of distributing private information about me go against that? So would that immunity not exist?

Could you spell out for us a little more clearly and precisely the hidden cases in which immunity would not apply, if there are any? I would like to see whether the risk that most privacy experts have told us about in section 487.0195(1) is as great as they say.

If any other witness has an opinion that they would like to share with us on this matter, please feel free to do so.

● (1135)

[*English*]

Mr. David Fraser: Thank you very much, and thanks for asking me those two particular questions.

In our Canadian criminal law, there are a number of circumstances where law enforcement agents can go to a justice of the peace or a judge and they have to satisfy whatever that burden of proof is in order to get some sort of compulsory instrument, which can be a wiretap order, or it could be a search warrant or a production order.

There are different thresholds for those. It generally depends upon the intrusiveness of the measure. Something like a search warrant to enter your house—for law enforcement agents to be authorized to, for example, break down your door—they have to have a very high standard of understanding. They're doing this on good information, very reliable information that they have reasonable grounds to believe—not just suspect, not just think—that a crime has been, is being, or will be committed and that the order is necessary in order to get that information.

In other sorts of compulsory processes, the standard is going to be lower on the understanding that the nature of the information being obtained is less intrusive. There's a difference between going into somebody's bedroom and going into their safety deposit box at a bank, for example. It recognizes that discretion.

What I was suggesting with respect to this transmission data recorder is to recognize that if it's fine, and the courts have upheld reasonable grounds to suspect, for telephony metadata, telephony signalling data, I don't think, because of the different nature of the information, that this reasonable grounds to suspect is appropriate.

As well, it might not actually survive court scrutiny because of the nature of the information that's being disclosed. It's never, in these sorts of circumstances, simply a matter of black and white. You end up in shades of grey.

The second question that you asked and I'm grateful for was the question related to immunity, and particularly you flagged the issue with respect to the charter. It takes two to tango in this sort of circumstance where the law enforcement officer would go to the telecommunications service provider and ask for the information. Under the Criminal Code, it's fine. Police can ask for anything; whether they're lawfully entitled to compel it, they can ask for anything from anybody. They're asking for the telecommunications service provider to voluntarily hand over that information.

The telecommunications service provider really doesn't care about the charter in terms of informing their decision-making. The charter applies to the police officers. It applies to whether or not the evidence that's gathered will be admissible in court, but the telecommunications company isn't involved.

So they're going to ask themselves a couple of questions. Am I legally able to hand this over? Am I legally prohibited from handing this over? And is there any civil liability that I could incur?

So one of the challenges we have is this. We don't have it in front of us, but Bill S-4 is going to amend PIPEDA, the Personal Information Protection and Electronic Documents Act, and in particular paragraph 7(3)(c.1), which is currently being reviewed by the Supreme Court of Canada with respect to whether or not, and under what circumstances, Internet service providers can hand over customer information on a non-warranted, non-judicially authorized request.

I understand that certain Canadian telecommunications companies do hand over that sort of information without a warrant. Their decision-making has been guided by the reading of an extremely ambiguous portion of that act, which allows a company—because we know the police can ask anything—to disclose information without consent to a law enforcement agency if they say—it's not under oath, it's not verified—that it relates to an investigation of a contravention of the laws of Canada or province, or a breach of an agreement, and they've identified their lawful authority to obtain the information.

So what the Supreme Court of Canada is considering is this question of lawful authority. Some telcos and police agencies take the view that simply policing duties is lawful authority to obtain the information. Others take the view that it's not sufficient. Lawful authority needs to be something else, something that is compulsory.

Some telcos err on the side of caution. Some err on the side of handing over information to the police agencies. But when they're asking themselves whether or not they should do that, in the background is also whether or not they could be sued for it. Handing over information where they're legally not compelled to, but there's a privacy law and a privacy interest at stake, could amount to something called an intrusion upon seclusion, which the Ontario Court of Appeal said you're entitled to damages for if that happens.

So I think what's happening here is that this provision has been put in here in order to make sure, in order to take that out of the equation —

The Chair: Mr. Fraser, the question and answer period is only five minutes long.

Mr. David Fraser: My apologies.

The Chair: I'm sure there will be another question for you to follow up with for the rest of your answer.

Mr. David Fraser: My apologies. I'm used to lecturing at a law school.

The Chair: Mr. Dechert.

● (1140)

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

Thank you to each of our guests for being here today and sharing their expertise with us.

Mr. Fraser, I'd like to start with you. You mentioned in your opening remarks that you were pleased to see the creation of a Criminal Code offence for the non-consensual distribution of intimate images. Then you gave us your views on some of the investigative powers that are covered in Bill C-13.

Are you familiar with the report of the cybercrime working group, which is made up of experts from each province and territory? Are you familiar with their recommendations?

Do you agree with their recommendations with respect to police investigative powers?

Mr. David Fraser: I do, by and large. As long as it's coupled with the appropriate judicial oversight, I think the police should have the appropriate tools to investigate crimes whether they happen online or offline.

Mr. Bob Dechert: Are you familiar with the facts of the Amanda Todd case?

Mr. David Fraser: I am.

Mr. Bob Dechert: We know that the matter is before the courts, and we don't have all the information. However, we do know that an individual who is resident in the Netherlands has been charged. We have heard that the information that led to that person's arrest and the subsequent charges was provided by U.S. authorities.

Are you familiar with U.S. authorities' powers in terms of investigation of these kinds of crimes?

Mr. David Fraser: I'm not a U.S. lawyer, but I have certainly been involved in cases in which U.S. authorities have been involved.

Mr. Bob Dechert: For example, we were told by the Department of Justice officials last week that U.S. authorities have preservation powers with respect to Internet data. They have had that power for 15 years or more. That power does not exist currently in the Canadian Criminal Code. Do you think it should exist in the Canadian Criminal Code?

Mr. David Fraser: I do. The only condition I would add to it...or "condition" isn't the right word. As it's written in Bill C-13, it allows a law enforcement officer who requires the preservation of that data to impose any conditions that officer deems fit, which gives too broad and open-ended a level of discretion to the law enforcement officer.

If they want to couple that with a gag order or something else like that, that should come from a judge, in my view.

Mr. Bob Dechert: But in terms of preservation orders, do they not need to meet a higher threshold with respect to disclosure of that information?

Mr. David Fraser: Ultimately it's a matter of asking them to preserve the information so the law enforcement agency has the time and the opportunity to get the appropriate warrant, and it makes perfect sense.

Mr. Bob Dechert: Okay.

If we had another case like Amanda Todd.... And my understanding is that this individual tricked her into providing an intimate image. He then went back to her with the threat that if she didn't provide even more revealing intimate images, he would post the first image to a Facebook site. He knew through her Facebook site online who her friends were, where she went to school, etc.

Without the provisions that Bill C-13 is seeking to add to the Criminal Code, how would a police officer, had Amanda Todd or somebody like her been able to come forward after the first image was provided but before the subsequent intimidation, have been able to find that individual and prevent him from posting the first image and threatening her and forcing her to provide any subsequent images?

Mr. David Fraser: Specifically you're asking about that in the absence of the availability to order preservation.

I'm in agreement with the preservation powers in the bill. Currently, it's my understanding, most telcos do voluntarily cooperate. I know I've been involved in civil matters where we have required or have requested the preservation of information in order to then get a subsequent court order to identify an individual, including in the case we took to the Supreme Court of Canada, and the telcos were cooperative.

Information online—these log files—tends to expire after 30, 60, 90, or 180 days, so if you can get that order within that interval of time, you're generally okay. It's when you end up with a longer and more open-ended investigation that it's more critical. But I do agree that it's an important tool to have, and it's not a particularly intrusive one as long as it's not coupled with a broad discretion to put conditions on it.

Mr. Bob Dechert: You mentioned that the Internet data that is provided in these sorts of situations includes information often about the whereabouts, the exact location, of the individual, especially when they are using a mobile device.

Do you think it's important that the police have that power in order to try to apprehend the person who is threatening to use those images for an illegal purpose?

● (1145)

Mr. David Fraser: In my view, the police should be able to obtain just about any information other than privileged information, as long as it's coupled with the appropriate judicial authorization. Absolutely.

Mr. Bob Dechert: So that information that includes the location of the individual can be disclosed, Bill C-13 actually raises the threshold to reasonable grounds to believe—is that correct?—in what's called a tracking warrant.

Mr. David Fraser: There are a whole bunch of moving parts, but without looking at it, I would agree.

Mr. Bob Dechert: Do you think that's reasonable?

Mr. David Fraser: I believe so. Yes, I do.

Mr. Bob Dechert: What other powers do you think the police need in order to properly investigate these kinds of cases? If you disagree with any of the cybercrime working group suggestions, maybe you could highlight those for us.

Mr. David Fraser: I don't have them in front of me, but I do believe that the general production order power, a general warrant power, and specific wiretap orders generally will cover off most information that's necessary in these circumstances. Then we have these additional ones with respect to the installation of tracking devices and things like that. But really, the tracking device does nothing for most cybercrime. That relates to crime that takes place in three dimensions in the real world.

But I do expect that this does cover off most of the investigative tools that are necessary, and as I said in my opening statement, I'm glad that they are all coupled with judicial oversight. The only question for tweaking is that in some cases, given the nature of the information, is reasonable grounds to suspect, compared with reasonable grounds to believe, the appropriate threshold?

The Chair: This your last question.

Mr. Bob Dechert: Okay.

Let's compare a non-Internet type of traditional sexual assault crime versus the cyberbullying situation. If a person sees somebody attempting to, or reasonably suspects that somebody is about to, commit a sexual assault, do they have the right to disclose that information to the police?

Mr. David Fraser: So if it's somebody walking down the street and—

Mr. Bob Dechert: Let's say it was in a private residence. You saw somebody in that private residence doing something that you thought would lead to a criminal sexual assault.

Mr. David Fraser: I would pick up the phone and call 911.

Mr. Bob Dechert: Fair enough. And would you suffer any liability if you were wrong?

Mr. David Fraser: No.

Mr. Bob Dechert: So what's different about the potential for a cybersexual assault, as Ms. Guthrie frames it, if you see something, and you have information that you believe may lead to this kind of an assault? Should you be held civilly liable if you're wrong, even though you could possibly—

The Chair: Mr. Fraser, you don't have to answer that question. He's used up his time.

I was generous with both, and I'm going to be generous with our Liberal colleague here with the same amount of time. There is lots of opportunity to ask that question to follow up on the question that was just asked.

With that, thank you for those questions and answers.

From the Liberal Party, Mr. Casey, the floor is yours.

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

Thanks to all the witnesses.

Mr. Alhattab and Madam Guthrie, I particularly appreciated your comments with respect to restorative justice. I do think that's something that should appear much more on the agenda.

I share Mr. Fraser's view that the major problems with this legislation relate to the reincarnation of Bill C-30. Ms. Guthrie spoke to that at some length as well.

Mr. Fraser, I want to focus in on the section that you referenced, proposed section 487.0195, and on the warrantless, secret, non-consensual, voluntary disclosure of information. You spent some time talking about the types of information that are available on a reduced legal standard. I know that when you listed that information you weren't talking about the stuff that can be obtained without a warrant.

Just for the benefit of everyone here, what is available without a warrant? What can be lawfully voluntarily disclosed by telephone companies under the protection of PIPEDA?

● (1150)

Mr. David Fraser: I tend to disagree with the interpretation of the statute that says lawful authority is anybody with a badge. Let me tell you what is routinely disclosed without a warrant in these sorts of cases. Many of these are reported in court cases. You just have to go the legal databases and search for PIPEDA requests.

The investigating officers have an IP address. They're able to obtain an Internet protocol address related to somebody of interest, and that can be because that person is believed to be sharing child pornography. Most of your activities that take place online expose your IP address to any computer that you connect to. So they have that IP address. They don't know who it is. They can determine, through public databases, what is the Internet service provider. They can go to that Internet service provider and say, "We have an IP address. We want to know who it is. We don't have enough information to convince a judge, but we're going to tell you that it relates to a child exploitation investigation or otherwise."

Some Canadian telcos, if that request is in writing, will hand over that information. Other Canadian telcos will say to come back with a warrant because they're not comfortable that they're allowed to under PIPEDA. That's essentially the nub of it. None of them, to my knowledge, will hand over content. If you say "I want the content of the e-mail inbox of Joe Blow at whatevermail.com", they're not going to get that without a warrant. We've heard in the debates over Bill C-30 that this is not private information. In fact it is. I believe you have a privacy interest in your activities online, and I think most Canadians would agree. Most of the debate, I think, turns on that particular question.

Mr. Sean Casey: The minister appeared before committee last week and said this immunity that is contained in this section is not new. It's been there since 2004. It's enshrined in the common law. It's also part of the Criminal Code.

Can you respond to that? Is this something that is new? Is this something that should be of concern to those who value their privacy? Is it a further encroachment above what was there before Bill C-13 comes into place?

Mr. David Fraser: My first question when I saw it and heard the debate about it is that if this is already the law, why are we putting it in the law? It really does beg the question. It must be doing something.

When you pull it apart and look at all of its different pieces, it says that you will have no liability for doing something that you're not prohibited from doing; it doesn't say you'll have no liability for something that you're lawfully able to do.

Words matter in legislation. I don't need to tell anybody in this room that's the case. But in fact that difference in words actually has a significant impact. It allows the person requesting the information to say to the telco that nothing'll happen to you if you hand it over; just hand it over.

In privacy you're talking about matters of degrees, and you're talking about expectations and things like that. So in theory, to follow the logic of the other arguments, a law enforcement agency could ask a telecommunications company, please give me the names, addresses, phone numbers, IP addresses, and e-mail addresses of every single one of your customers. We can lawfully ask that. Under that extreme reading of PIPEDA, they could hand that over. I would say they would be civilly liable for intrusion upon seclusion under the law for doing that. They're not prevented from it or prohibited from it according to that reading of PIPEDA.

So that would allow them to do that, and I'm not sure we want to encourage that sort of behaviour. If you can convince a judge that you're entitled to that for a lawful purpose, then absolutely, fill your boots, you're entitled to it. But that sort of behind the scenes, in the shadows, with no accountability causes me great concern.

Mr. Sean Casey: Let's come back to the accountability aspect. So I, as a customer of a telephone company, have no opportunity to provide consent to the release of my private information upon request by anyone. I also have no right to know that my information has been disclosed to anyone.

I asked the minister about that, and he said, well, that's a contractual matter as between the telephone company and its customer.

What are your views on that?

Mr. David Fraser: That would be a misreading of PIPEDA. If law enforcement or anybody asked for information, and it's provided under paragraph 7(3)(c.1) of PIPEDA, and the customer then says "Did you hand over my information?", the telco, the service provider, has to go to the law enforcement agency and ask them for permission to hand over the information. It has nothing to do with the terms of service with the customer. It's the legislation that imposes the gag order in that particular case.

There are thousands of requests for customer information. We heard the number of 1.2 million last week. In the vast majority of those cases, unless charges are laid and the information is part of the crown disclosure, the individual never finds out. They have no idea. So all of this happens in the shadows, and I think accountability to the person who it concerns is of prime importance.

● (1155)

The Chair: You have a few seconds left.

Mr. Sean Casey: Isn't it true that there actually aren't individual requests? What actually happens is the telephone companies and Internet service providers set up a separate file that they give law enforcement the authority to access. So there actually aren't individual requests. They've made their own protocol as to what they can have at.

Is that not the way it actually plays out?

Mr. David Fraser: My understanding is that of that number of 1.2 million, a large portion of them relate to a special law enforcement database that is essentially the same as Canada 411, where it's non-private information. It's stuff that would already be in the phone book, but it's just immediately up to date and it's accessible.

I'm not so worried about that lump of requests. I'm much more worried about the other more intrusive ones that are hidden within it that we don't have any transparency into.

The Chair: Thank you very much for those answers.

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

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

Thank you to all of the witnesses for coming and testifying today, and thank you, Ms. Guthrie, from faraway Toronto.

I want to follow up on Mr. Dechert's question. He didn't get the answer he was looking for, not because you couldn't provide it but because you didn't get the chance. He was giving you the example of, look, somebody witnesses a sexual assault and picks up 911; how does that differentiate from an IP provider voluntarily giving some information? Why would there be liability on one and not on another? I don't see any distinction, really. Is it a question of the reasonable expectation of privacy or....? Guide me here.

Mr. David Fraser: I'm happy to, but I don't think the two are analogous at all. The reason is that if I as a private citizen see a crime taking place, I don't have a legal duty to, but I certainly can pick up the phone, call 911, and report it.

Mr. Robert Goguen: But if you suspect it.... I mean—

Mr. David Fraser: Or even if I suspect: any private citizen can do that. Because I'm not subject to PIPEDA. I'm not an organization subject to privacy legislation, and I don't have a contractual relationship with the people in that room who say, "I will keep your information private." What you're talking about, on the other hand.... Also, if I call 911, that's at my own volition. That's me deciding to do so, and actually, the law doesn't compel me to; I can perversely stand there and watch it happen. But that's neither here nor there.

When it comes to law enforcement knocking on the door of an organization that's subject to privacy legislation and asking them to hand over information voluntarily, they have to ask themselves: "Can I do this? Can I do this under my terms of agreement with my customer? Can I do this under the telecommunications legislation? Can I do this under privacy legislation?"

If everybody in this room has a problem with privacy legislation and a problem with that scenario, then debate it and deal with it in the privacy legislation, rather than in something that we're being told is just restating the status quo but in fact changes the status quo with these sorts of things.

Mr. Robert Goguen: As it stands, there's nothing that can compel the provider to provide the information. They can very well say no, that they're not interested in providing that, so please go get your warrant. Correct? There's nothing that engages them to have to provide this, right?

Mr. David Fraser: The provider can do that and, in my view, the provider should do that, but again, it's an important distinction between who is reporting the crime and who is being asked for the evidence.

Mr. Robert Goguen: All right. You've clearly set out the difference. That's good.

What about the agreements between the customers and the providers? To your knowledge, are there any agreements that providers use—you seem quite versed in it—that would authorize them to disclose something that might be illegal?

Mr. David Fraser: Certainly, and again, the distinction is when the police request it rather than at the initiative of the organization.... In a number of the cases that are reported where the police have asked for customer information without a warrant, when it finally goes to trial, it's not the telco that's on trial in these cases—

● (1200)

Mr. Robert Goguen: Correct.

Mr. David Fraser: —it's the accused, with respect to whatever their activities were. The crown will point to the terms of use of the Internet service provider if it's to their benefit to do that.

In some cases, some Internet service providers put in black and white in their terms of service that they reserve the right to provide information to law enforcement under certain circumstances and that may be triggered, the idea being not because it has anything to do with the service provider, but that it reduces the expectation of privacy on the part of the individual with respect to their charter rights, with that section 8 of the charter being engaged.

It's a bit of a legal fiction, because I don't know whether anybody in this room has actually read the terms of service they have with their service provider—

Voices: Oh, oh!

Mr. Robert Goguen: That's why I asked.

Mr. David Fraser: —but certainly it has been pointed to as a basis for diminishing that expectation. I guess it takes three to tango, in that case.

Mr. Robert Goguen: Yes, and I wonder if that would suffice to exempt them from civil liability. Probably not.

Mr. David Fraser: It would depend upon the form of liability. Certainly, one can consent, as long as it's informed consent, to what would otherwise be an intrusion upon your seclusion. If you agreed that somebody could do something to you that would otherwise be an invasion of your privacy, it would be very likely that this would be the defence set up with respect to any sort of lawsuit. It wouldn't be immunity per se, but it would be that your case would lose, so it's effectively the same result.

Mr. Robert Goguen: Maybe because of the contractual provisions the immunity may not even be required, depending on how strong the wording is.

Mr. David Fraser: It may be, and if one wants to accomplish this result, as I said, one could amend PIPEDA, or one could maybe convince the telcos to put in their terms of service that this information will be handed over in bulk, which I don't think Canadians have an appetite for.

Mr. Robert Goguen: Your approach is very balanced. I see that you're not against the police powers and the preservation of information as long as the level of intrusion is matched by some amount of supervision. I think that's well reasoned.

I was curious about your comments on, say, an image being given to a third party, and they have no way of knowing.... You said that the standard was reckless, that it was too low. What's your suggestion on what these standards should be?

Mr. David Fraser: Let me just flip to exactly what I said in my opening statements. I think it needs to be that the person knew or ought to have known that the individual in the images did not consent. I think that in a lot of cases it is the initial sharer of those images, or somebody who knows the victim, where it is in fact most egregious and probably crosses the line into a criminal violation.

Mr. Robert Goguen: I guess your comment is that the volume of stuff that's circulating on the Internet.... I mean, that standard of recklessness is far too low because of the sheer volume of what's taking place on the airwaves, I guess.

Mr. David Fraser: No, I think my conclusion actually comes down to the blameworthiness of the conduct.

Mr. Robert Goguen: The guilty mind.

Mr. David Fraser: The guilty mind: somebody who knew, somebody who was in fact betraying a trust. That in my mind reaches a level of criminal culpability.

Somebody who has no idea, and no reason to know? You don't criminalize that sort of conduct.

Mr. Robert Goguen: That's fair enough.

Thank you.

The Chair: Thank you for those questions.

Thank you for those answers.

Our next questioner is Madame Boivin.

[*Translation*]

Ms. Françoise Boivin: I am going to let Ms. Guthrie get into the discussion. We would not want Toronto people to get bored.

I seem to remember reading some comments from you on the burden of proof in terms of consent. They want to amend section 162 by adding subsection 162.1(1), which reads as follows:

> Everyone who knowingly publishes, distributes, transmits, sells, makes available or advertises an intimate image of a person knowing that the person depicted in the image did not give their consent to that conduct, or being reckless as to whether or not that person gave their consent to that conduct, is guilty:

What interests me in that section is the burden of proof. Normally, the Crown has to provide all the evidence of an offence. I seem to remember reading something to the effect that the accused would have the burden of establishing that he obtained consent and that he took the trouble to find out if the person in question consented or not. Should that be specified in an amendment?

[*English*]

The Chair: The floor is yours, Ms. Guthrie.

Ms. Steph Guthrie: It was once my position that if the accused cannot furnish proof that they had consent to share the image publicly, they should then be subject to whatever legislation is designed. I would say that since I wrote that, my position has changed, and I'm of the same mind as Mr. Fraser on this issue.

I do think the "being reckless" clause is a little bit dangerous; the best way to design this legislation would be to rephrase it to something along the lines of "known or ought to have known" or "a reasonable person would assume" that the person did not give their consent to that conduct.

The reason is that you want to include people, for example, who might share an image from a website that is specifically created and marketed to share non-consensual images. Sad to say, there is quite a market for this. If someone visits a website that has marketed itself as a place where you can find images of people who didn't consent to the images being shared, well, if you share from that website, even if you don't have direct knowledge of the subject's consent, you ought to know that they didn't consent.

So the wording that Mr. Fraser outlined is what I would now suggest.

● (1205)

Ms. Françoise Boivin: It should be amended, in that sense.

[*Translation*]

Thank you, Ms. Guthrie.

[*English*]

I will go back to you, Mr. Fraser.

[*Translation*]

Could you specify the type of amendment you would like to see to section 487.0195(1), when it is done without authorization or voluntarily? Should people have to be informed in those cases only?

It reminds me of the time when our committee was studying Bill C-55 about electronic surveillance. Perhaps other members of the committee will remember. The Supreme Court said that there was a deficiency in the Criminal Code in that respect because people never knew when they had been subject to electronic surveillance.

What is being said today is all well and good, but a number of cases will not result in charges at all. Information may be circulating anyway. Should there be specific provisions for all the cases in which charges have been laid? In those cases, we would end up knowing because the Crown would be forced to disclose the information. What kinds of provisions should we include in Bill C-13 to make sure that people are informed, within a reasonable timeframe, that they have been under electronic surveillance? If I remember correctly, I think that a period of 90 days was considered.

Should there be an automatic notification so that people find out that their information has been circulated, whether or not it came after a warrant?

[*English*]

Mr. David Fraser: Thanks very much for the question.

I agree that in virtually every circumstance in which government or law enforcement agencies obtain the information about an individual when that individual is not informed at the time, they should be informed within six months—six months seems to me a reasonable interval of time—unless the law enforcement agency or government agency can convince a judge that providing that notice at that time would in fact impede a current, ongoing investigation.

I'm not as concerned about cases in which this information is disclosed and obtained by law enforcement and then charges result. That ends up seeing the light of day, in a courtroom or otherwise, and so there is accountability and transparency in that case.

What I am concerned about, and think Canadians should know, is how often information about Canadians is obtained, with or without a warrant, that never in fact leads to charges. That kind of situation could lead, if we take a close look at it, to their maybe getting information more often than they should. Maybe they're getting information about a huge number of people, such that in fact it amounts to fishing expeditions whereby they're going to catch a couple of bad guys, but it's too much.

I think it's critical that everybody around this table, everybody in this room, but also every Canadian have the information in order to properly understand what's going on, so that we can have a proper debate on it. We've seen very adamant and strong positions over the last couple of years. We've had Bill C-30, we've had the revelations about the Canada Border Services Agency, this 1.2 million—we've seen the amount of ink that's been spilled in the interest of these topics. But at no time does everybody actually have the information in front of them to properly understand. It just becomes fodder for arguments based on doctrinaire positions.

If we knew and if individuals knew, then we could actually have a much more informed and better discussion about it, leading to better laws, leading to appropriate oversight, leading to appropriate police powers in all of these circumstances.

I'm a very strong advocate of transparency, and that includes not just aggregate numbers, but individual notification.

The Chair: Thank you for those questions and answers.

Our next questioner is Mr. Wilks.

Mr. David Wilks (Kootenay—Columbia, CPC): Thank you very much, Chair, and thanks to the witnesses for being here.

I want to focus my questions in on the authority or the police powers as they exist today as opposed to what Bill C-13 will bring to police powers. I use my knowledge and my background with the RCMP. Having been so fortunate to be an affidavit for and the author for a part VI, I can tell you, and you are probably aware, that it's not a fun ordeal to go through.

Let's take it right back to the start of an investigation. We can use either a sex crime or a drug crime by way of example, because those are the two that normally are going to go down the road of an intercept, historically.

If I go to Bell, Rogers, Shaw, Telus—whoever it is—as a police officer, would you agree that the first thing I don't want to do is jeopardize the investigation? Would you agree that I don't want to jeopardize the investigation?

● (1210)

Mr. David Fraser: I would expect that as a law enforcement officer you do not want to jeopardize your investigation.

Mr. David Wilks: That's correct. So let's take it to the next step.

Although I would suggest that most police officers, including me, are not quite familiar with PIPEDA, we're quite familiar with how far we can or can't go. We do know that if I go to you, let's say, and you're with a telecommunications provider, I can say that I'm investigating so-and-so and I know that you have in your possession information that may assist us with that investigation.

I can tell you from personal experience that I never asked for the information. What I did ask was that you not destroy it or not move it. But under the lack of legislation that we have right now, you can't; it's basically voluntary. That's what it is.

So when we start talking about voluntarily providing information, the reality is that there's nothing in place right now to assist the police to better clarify or better insulate them and the telcos from the ability to preserve information. There's just nothing there.

Mr. David Fraser: Absolutely; I agree. There is no authority to compel somebody to preserve that information.

Mr. David Wilks: So it's done voluntarily.

Mr. David Fraser: That's my understanding.

Mr. David Wilks: So this legislation now, with form 5001, 002, and 003, goes from reasonable grounds to suspect, which the preservation order says "I want you to hold on to the information until I come back with a warrant".

Mr. David Fraser: Absolutely.

Mr. David Wilks: Right. There's nothing wrong with that.

Mr. David Fraser: No.

Mr. David Wilks: I just get a little confused when I start hearing about the 1.2 million pieces of data that are voluntarily...yet there is no other avenue for the police to do an investigation. There's just nothing. So this actually clarifies their ability to request the preservation of data as opposed to the voluntary preservation of data. It gives them some legitimacy to be able to go to the courts and say, "Listen, we followed the rules," because more often than not what happens—and agree or disagree—when you get to court there's a lot of presumption that goes on because there's lack of data for the police to be able to utilize and present.

So I just don't understand where we're concerned that what's going to be put in Bill C-13 would be any worse than what we have now.

Mr. David Fraser: I'm not saying I'm concerned about the preservation powers.

Mr. David Wilks: So when you refer to the 1.2 million pieces of data with regard to voluntary between what you're assuming is mostly law enforcement of one frame or another from a telco, what is your concern to which Bill C-13 would preserve?

Mr. David Fraser: I believe I've said a number of times I'm not concerned at all about the preservation. I think it's important to not confuse the preservation with the providing of the information. From what I understand, that 1.2 million has nothing to do with preservation. It has to do with information that has been provided.

I think we're all hampered by not knowing really what that 1.2 million represents. It represents some that were with a production order, some that were with an intercept order—

Mr. David Wilks: So would you agree that we're confusing the issue with the actual bill that's before us?

Mr. David Fraser: Certainly I think that there is a lot going on in this bill, and it might be easy to confuse the different pieces of it. Certainly there's a lot to be said for looking at each of them very closely.

A preservation order is of a different nature from a production order. I don't think there's any doubt. The preservation order is for any law enforcement officer who's authorized under the legislation to require somebody to just keep that information. I have a concern that it could be coupled with any conditions in the discretion of the officer, but to set that aside, it is different from an authorization to intercept, which is different from an authorization to require somebody to provide related transmission data, tracking data, and all those other things.

Just so I'm clear, and just so I'm well understood, hopefully, I don't have an issue with a preservation demand in and of itself. I think that it in fact is a deficit in our current system that should be addressed.

● (1215)

Mr. David Wilks: Would you agree that as the level of the investigation escalates, we go from reasonable and probable grounds to suspect, to reasonable and probable grounds to believe?

The Chair: That's your last question, Mr. Wilks.

Mr. David Wilks: And is it in an order that you are comfortable with?

Mr. David Fraser: It goes in a continuum and it's very circumstance-specific, but that continuum would relate, in my mind, not just to the progression of the investigation but to the intrusiveness of the measures.

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

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

[*Translation*]

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

I feel that this discussion shows how great the need is to divide this bill. To this point, I have not heard much about cyberbullying, but rather about access to information and some pretty technical things that, unfortunately, have nothing to do with what young people are experiencing at the moment and what people in the trenches perhaps need.

My first question is a technical one and it goes to all three witnesses. Should we establish the age at which a person could consent to images being distributed? At the moment, there is no such indication in this bill.

[*English*]

The Chair: All three have been asked; perhaps we can start with the Boys and Girls Club.

[*Translation*]

Mrs. Marlene Deboisbriand: Yes, we believe that there should be an age of consent.

What should that age be? In our opinion, that should be discussed with young people to get more informed opinion, to really get to know the different opinions they have, to really find out their perception of their own intentions and how the legislation could affect them. Determining an age of consent is important for us. It should be decided after having a conversation with young people.

[*English*]

The Chair: Madam Guthrie, would you like to respond?

Ms. Steph Guthrie: I'd like to clarify whether the age limit pertains more to the cybersexual assault component or to the state surveillance of personal information components.

The Chair: Go ahead, Ève, do you want to clarify that?

Ms. Ève Péclet: At what age would a victim be legally able to consent to the distribution of her or his personal images?

Ms. Steph Guthrie: Right. That's a very good question and an important one to consider.

I echo the representatives from the Boys and Girls Club in feeling that youth need to be consulted about this.

As a reasonable place to start, we can look at what ages youth are able to consent to sexual activity more generally in Canada. That would be where I would recommend starting the discussion, but I do think it would need to involve other discussions with youth.

I do think that in most cases the youth are not consenting to have the image shared publicly. I don't think you would see very many cases where young people are saying “But I'm old enough to have this shared with my entire school without my knowledge”. It is important to discuss an age limit, but I don't think in reality it would come into play very much in the way this crime actually plays out.

● (1220)

The Chair: Mr. Fraser, have you any comment?

Mr. David Fraser: I would echo those sentiments, and would only add that when it comes to somebody who is under the age of 18, those images would be child pornography images as well, which brings into play other legal tools for dealing with not just non-consensual but otherwise dissemination of those images.

[*Translation*]

Ms. Ève Péclet: My second question goes to Ms. Deboisbriand from the Boys and Girls Clubs of Canada.

In your presentation, you mentioned focusing on restorative justice. You also said that the key to that kind of strategy is education.

For the benefit of all the MPs here, could you talk about your experiences in the trenches, the experiences young people are having and what provisions on restorative justice you would like to see? It may not be included in Bill C-13, but it could be included in a future government initiative.

Mrs. Marlene Deboisbriand: Thank you for the question.

Let us talk about education first.

Most kids under 17 or 18 do not really understand the impact of their actions when the changes happen very quickly. We mentioned differences between the provinces in our brief. For example, we have the BGCC National Youth Council. Those kids are sending each other text messages every day. There are no differences across the country, no provincial or territorial borders.

There has to be a system of education through which kids can fully understand the impact of their actions and the consequences, in terms of sharing intimate images, and so on. For us, it starts with education.

In clubs that have a restorative justice system, it works on an individual basis. We sit down with the kids and try to see to what extent they are aware of their actions. Is he or she aware of the impact of the actions on the victim? Are they aware that the victims may not have consented to sharing the photos? A lot of questions are asked in that first interview.

We draw up a plan of what to do with the kid. The plan really is individual and it depends on the answers to all the questions. It might be to ask the kid to go to schools to talk about the experience, to explain how he or she dealt with the experience and what the consequences were. There can be broader reparations, such as hours of community work, likely with organizations that deal with challenges of this kind. It really is tailored and planned out to meet the needs of the client, the young person who has been accused.

[*English*]

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

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

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

Mr. Fraser, I just want to quickly go back to something. Where you're saying you have a problem with reasonable grounds to suspect is with respect to transmission data, and not in a preservation order. Is that where you have the problems?

Mr. David Fraser: Correct. Absolutely.

Mr. Kyle Seeback: My understanding is that when the standard is the lower standard, which is reasonable grounds to suspect, that's for specific, limited pieces of data as opposed to the general overriding section, which is proposed section 487.012. And under proposed section 487.012, it maintains the old standard, which is reasonable grounds to believe.

Am I correct in that distinction, and if I'm correct, why do you have a problem with the lower standard for very specific pieces of information? For example, routing information is designed to obtain information such as phone numbers, but it cannot include content; production for financial data is limited to basic financial information such as the account number and the date the account was opened.

● (1225)

Mr. David Fraser: I don't have my copy of the Criminal Code, so I'll assume what you said is correct.

My concern comes from this: that we are taking reasonable grounds to suspect, which is likely a fine threshold when you're dealing with routing information, basic bank account information, and we're now applying it to what's called transmission data, which goes beyond usual telephone systems and routing systems and things like that. So it is in fact exposing more information, more information about what the individual is doing. It's not just in terms of quantity, because I create more Internet signalling data in a day than I do telephone data that tells you more; it actually goes not specifically to the content of the communications but it's much more illustrative of the individual and therefore potentially more intrusive.

I think that if you're going to go up that intrusiveness scale, you need to go up the standard scale, or you need to reduce the intrusiveness and keep that threshold. To be absolutely clear, the transmission data only includes originating IP address, maybe ending IP address, the time of the transmission, and that's that. There's nothing related to protocol information, nothing related to the nature of the communication—not content, but the nature—and nothing related to that sort of stuff.

Mr. Kyle Seeback: If these were very specific snippets of transmission data and not incredibly intrusive pieces like the examples I gave, which are phone numbers, bank account number and when the account was opened, if it's limited like that are you comfortable with the standard of reasonable grounds to suspect?

Mr. David Fraser: Yes. If we can take the definition of transmission data and modify it such that it's at the same level of intrusiveness as those examples you just gave, then I would be satisfied with that.

Mr. Kyle Seeback: Thank you.

How much time do I have?

The Chair: You have four more minutes.

Mr. Kyle Seeback: Four more?

The Chair: Three more minutes.

Mr. Kyle Seeback: Three? Great.

The Chair: You have two more minutes.

Voices: Oh, oh!

Mr. Kyle Seeback: It keeps changing. Now one minute....

Ms. Françoise Boivin: Every word is worth a minute.

The Chair: You have three minutes.

Mr. Kyle Seeback: Okay.

To the Boys and Girls Club, the kind of work you're doing I think is great. Do you have any courses or information that you are passing on to young people as part of your own anti-bullying strategy, and if so, could you tell us a little about that?

Mrs. Marlene Deboisbriand: Yes, I'd be happy to.

May 7 is national belonging day, as we have chosen to call it, for the Boys and Girls Club. It's positive. The way to counter bullying is to talk about belonging, so we have a corporate partner with which we do a belonging day.

But on a more practical level, we have a number of sessions that are held in various clubs across the country, and we have 99 clubs. Some of them are in very urban centres, some of them are in very rural communities, so the programs offered in clubs vary from one community to the next. Most clubs do homework help and some snacks and all that kind of stuff. Those are common programs across the country.

More and more we're doing digital education with young children, and more and more we're starting them younger than ever before, so most clubs are starting the digital education programs as early as six years old, grade 1. When they come to after-school programming, educational programs are available to them and as the ages increase, those programs and what's covered in them intensifies obviously so we talk about sharing intimate images. We obviously don't do that with our six-year-olds, but we started doing it as early as with our 12-year-olds.

Mr. Kyle Seeback: You talked about some of your restorative justice programs and things like that. Do you find there's a particular profile for what we like to call a cyberbully, or is it just sort of any kid can end up making a poor choice? What's been your experience with that?

Mr. Fahd Alhattab: Personally, from what I've seen in some of the kids we work with, I guess maybe there is a distinction between a kid who sends out an image…not to try to bully, per se, but because he landed on this image, was talking to some friends about it, got pressure—"Oh, yes, send it to us"—and sent it out. For those cases, it's anyone and everyone, from as young as 12 or 13 years old sometimes to as old as those who are finishing high school and going into post-secondary.

For cyberbullying per se, I couldn't say I've profiled a certain individual or a certain type of person who would take this on and would be of that nature, but....

● (1230)

Mrs. Marlene Deboisbriand: The only thing I would add is that we often work with the bullies as well as those being bullied. Although there isn't a traditional profile of any kind, often these are kids who have had just a tough time, who haven't built up the confidence. It often stems from a lack of confidence, and it's a way to gain respect. It's many of the same patterns that lead young people to join gangs. It's a way to gain respect, it's a way to feel some strength, to feel some power.

So we work a lot with kids who we've identified as having some bullying...who themselves are being the bullies. We work with them to look at what's creating those behaviours and how to put that in reverse, if you wish.

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

Our next questioner is from the New Democratic Party, Monsieur Jacob.

[*Translation*]

Mr. Pierre Jacob (Brome—Missisquoi, NDP): Thank you, Mr. Chair. My thanks also to the witnesses for joining us today.

My first question goes to the representatives from the Boys and Girls Clubs of Canada.

Could you tell me whether you were consulted as Bill C-13 was being developed?

Mrs. Marlene Deboisbriand: Not really. We reached out to some extent and we had a few meetings, but I feel that the consultation was somewhat limited. However, we greatly appreciated the opportunity to present a brief on the bill.

Mr. Pierre Jacob: I see that you are working to develop appropriate programs for young people on cyberbullying. As I understand it, it is a work in progress. Has there been an increase in the resources you need across the country?

Mrs. Marlene Deboisbriand: You can see me smile. Yes, there has been an increase in the resources for those programs because the needs are increasing and changing very quickly. The additional resources mostly come from large corporate partners, companies, that are helping us with our work. Unfortunately, in no case has there been an increase in funding from any level of government.

Mr. Pierre Jacob: You mentioned affronts to privacy that Bill C-13 could give rise to. Could you tell us what your perception is there?

Mrs. Marlene Deboisbriand: My answer is along the same lines as my two colleagues who have testified today. For us the affront to privacy is the same for young people as it is for adults. The difference is that kids are less aware than adults of the fact that an element in the bill itself affects privacy. Most kids are not aware of it, nor are they aware of the flexibility that the bill establishes or of the possible repercussions on their privacy as teenagers or young adults.

Mr. Pierre Jacob: Thank you. You also mentioned the importance of education and of restorative justice. Could you talk to me about the importance of prevention as well?

Mrs. Marlene Deboisbriand: I talked about that with one of your committee colleagues just now. In terms of cyberbullying, we are doing a lot of work with kids who have been victims of it. But we are also working with kids who are doing the bullying themselves. In order to prevent it and to stop it from happening again, it is important to work with the bullies too.

Things are changing quickly. We are seeing a lot of cyberbullying among girls. Often people think that it is a phenomenon among boys, but it does not just affect boys. Girls are not just victims of bullying, they are bullies too. More and more, we are working with girls as well as boys, basically.

For us, education is, of course, directed at the young people themselves. However, an element of the education is for the parents and families of those young people. We are often working in areas with lots of newcomers. The parents are not always as technologically advanced as their children are. So it is important to do a lot of work with everyone around those young people so that they understand the consequences of bullying, their actions, sharing photos, and so on.

So our approach to education involves everyone around the young people, including the young people themselves.

● (1235)

[*English*]

Mr. Fahd Alhattab: Just quickly, to speak to the education point, the reason we really focus on education is that we focus on the root causes of why someone would cyberbully. Why would somebody send a photo? Why would someone feel pressured to share the photo?

The example we use with a lot of our youth workers is this. Let's say I give you a very complicated math problem and tell you that if you don't solve it, I'm going to punish you. If your skills aren't there, you won't solve it, no matter what the punishment is and no matter how severe it is. Even if I say I'll give you $1 million to solve this math question, the likelihood is that if you don't have the skills, you won't solve it.

It's the same problem. A lot of times it's a lack of skill. It's a lack of understanding and a lack of education that a lot of these kids have, and no matter what we inspire them with or what the consequences may be, if that education piece is missing, it won't change anything.

[*Translation*]

Mr. Pierre Jacob: My next question is for Mr. Fraser.

Could you sum up for me, in order of priority, the problems with Bill C-13 that you mentioned to us in your presentation?

[*English*]

Mr. David Fraser: I think it's probably dangerous to ask me to summarize Bill C-13 or my concerns.

An hon. member: You have one minute.

Voices: Oh, oh!

Mr. David Fraser: Thank you very much.

This is a complicated issue that we're looking at. The cyberbullying part is a complicated phenomenon with a lot of moving parts. We've heard a whole lot of nuances. Police investigative powers is a complicated question because we need to make sure that the balance is struck right. The police need to be able to do their jobs. They have an absolutely critical role to play in our society.

We also have fundamental freedoms that are inherent in how we want to organize ourselves in this society. So in both cases, it's a matter of getting the balance right. Cyberbullying, the distribution of intimate images without consent in order to harm somebody, harms people and causes problems, and we want to, in the right circumstances, punish the right people.

In the second half of the bill, the second three quarters of the bill, we want to actually give the police the appropriate powers in the right circumstances with the right oversight to do that. We're dealing with some complicated, nuanced questions with a lot of moving parts—this fits together with child pornography, and the production order powers fit together with search warrants and other things like that—so this committee has a daunting task in front of it, over the next probably five weeks or so, to try to get both of those parts right.

I would suggest you spend five weeks on one, and then five weeks on the other, but that's going to ruin your summer.

Voices: Oh, oh!

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

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

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

My first question is for the Boys and Girls Club. One thing that I think we haven't spoken a lot about today, and that I thought you could provide insights into, involves the impacts of cyberbullying and how frequent it is.

I think Ms. Guthrie spoke about how increasingly frequent it's becoming, but I'm sure you see that in your clubs.

Perhaps you could speak to, one, how frequent it is, and give us insights from what you've observed; and two, the impacts it has on youth.

Mrs. Marlene Deboisbriand: Do you want to start?

Mr. Fahd Alhattab: Yes.

We actually did a fun project with some of the youth. They created a video on cyberbullying and anti-bullying within their clubhouse, which was a great project to get them to learn more about it. But what we came to realize was that a very high percentage of youth, close to 80%, are affected by cyberbullying.

There's the fact that we have our cellphones with us all the time. We like to discourage them to use a cellphone at the Boys and Girls Club, but even at the Boys and Girls Club, when you feel welcome and you're at a place where you belong, you could be receiving messages that are affecting you, and that are affecting you in your physical place, when you're receiving them virtually. From being at home, from being at clubhouses and being at schools, which could all be very nurturing environments and have very strong role models, sometimes the difficulty is in their pocket, with the cyberbullying.

It affects the children and the youth in their schooling. It affects them in their relationships with others. I think it goes to the point my colleague made about confidence. Confidence is hard to measure, but you can see a huge difference between the kid who's confident in themselves and their abilities and the kid who is constantly being bullied and doesn't have that same charisma to them.

● (1240)

Mrs. Marlene Deboisbriand: The only thing I would add is that the numbers are a little misleading. Again, it depends on how you define “cyberbullying”. In the context of this bill, there is a definition. When we use the 80% or 85% number in terms of children and youth affected by cyberbullying, we are no longer talking about sexting and sharing of intimate images. We're also talking about people just being mean.

When I talked about girls being the perpetrators, often it's not about sexting or about sharing images; it's about being very mean. It's what some of us, depending on our age, used to experience in the schoolyard. Now it's with you 24/7, because it's in your pocket, your purse, or your knapsack. The numbers can be pretty staggering when you include just being mean versus....

In our clubs we tend to see less of what I would call extreme cyberbullying, what our colleagues referred to as sexual assault online. Those kinds of things are less prevalent, because our kids are in our clubs and are in a safe place and are busy experiencing programming. So they tend to have smaller numbers.

Mr. Patrick Brown: I have a follow-up question for Ms. Guthrie.

You mentioned that in the bill there were aspects toward cyberbullying that you really liked. Your concern was that there was too much in the bill, but I wanted you to highlight the parts you liked. I think it would be helpful to know the parts of the bill that you thought were very helpful.

Ms. Steph Guthrie: First of all, I was glad to see that the provisions around cybersexual assault were added adjacent to “voyeurism” in the Criminal Code. I do see a lot of parallels between these two types of behaviour. I think they fit together, and I think that was an appropriate place for it.

I also appreciate that it's written into the bill that the subject of the image needs to have.... If they had a reasonable expectation of privacy at the time the image was captured, in addition to at the time the image was shared or the offence was committed, I think that by having these two things in there, you're covering a lot of bases and making it relatively airtight.

I liked a lot of things about it. It was primarily the “being reckless” as to whether someone gave their consent that I took issue with.

The other thing that I think could potentially be a problem is in proposed paragraph 162.1(2)(c). I am concerned about the latitude with which a judge might interpret whether a subject had a reasonable expectation of privacy at the time the offence was committed.

As an advocate in this area, I have seen a lot of people try to pursue justice for these things, whether through harassment legislation or through child pornography legislation. Having law enforcement officers.... I've seen it, certainly in the States and potentially here, as well. In some cases, even judges will just decide, because they personally think you shouldn't have shared those images in the first place, you wouldn't have had a reasonable expectation of privacy at the time the offence was committed. So I think there's potential for it to be interpreted.

Mr. Patrick Brown: Ms. Guthrie, I appreciate your perspectives on the judiciary and law enforcement, but I want to ask a follow-up question. Are you aware of the federal-provincial-territorial report that was released in July of 2013 calling for additional measures? In particular, it called for giving law enforcement better tools to deal with the gaps.

I'm wondering if you are aware of the report and if you support the recommendations that were made in that report.

● (1245)

Ms. Steph Guthrie: I actually have not read that report. I'll have to check it out. Thank you for flagging that for me.

I think for me, a lot of the time, the issue is less with the tools that are available to law enforcement and more with the specific attitudes that individual law enforcement officers hold and potentially attitudes that are encouraged by the culture of law enforcement that often blames female victims of sexual offences for the offence rather than the perpetrator.

The Chair: Thank you for those answers.

Our next questioner, based on the schedule, is from the Conservative Party again, Mr. Dechert. I'm going to try to hold you to five minutes.

Mr. Bob Dechert: Okay. Thank you, Mr. Chair. I'll try to be brief.

Mr. Fraser, I'm still concerned and confused, frankly, about your concern about the release of an ISP provider or another entity from civil liability if they voluntarily disclose some information in response to a request from police authority. Forgive me, I'm more of an analogue than a digital kind of guy, as I suspect most parents are in Canada.

Let me phrase it in a way that I understand. If I see some suspicious activity around my neighbour's house, I can pick up the phone, dial 911, speak to the police, and tell them that perhaps someone is trying to break into my neighbour's house. They investigate. I'm wrong. It's the gardener. It's a repairman. Do I expose myself to any civil liability by doing that?

Mr. David Fraser: If you acted in good faith, no you don't.

Mr. Bob Dechert: So if the police come to me and ask me if I've noticed any suspicious activity around my neighbour's house recently, and I mention that I saw somebody acting suspiciously there yesterday, that there was a car parked in the driveway, and I give them the licence plate number, which I noted down, they go and they find that person. He was not in fact attempting to break into the house, but again, he was the repairman or the gardener, etc. Am I civilly liable for providing that information to the police when they ask?

Mr. David Fraser: No you're not, for two reasons. First—

Mr. Bob Dechert: I'm short on time, so let me get to the next point because I think it's more important.

Let's go into the digital world. Somebody like Amanda Todd unfortunately gives up a picture to somebody, consensually probably, but she was tricked—

Mr. David Fraser: Coerced: I wouldn't call that consensual.

Mr. Bob Dechert: She's a young person. She doesn't know who she's dealing with over the Internet. She gives an intimate image. At that point in time, she steps forward and expresses her concern. She says that she gave somebody an image and that she's not sure what they're going to do about.

Under Bill C-13, the courts are provided with the power to essentially impose an injunction against further use of that image and to order the destruction of that image. How can you do that if you don't know who has that image? She goes to the police. The police go to her ISP provider and say, "Can you tell us where that message came from?" If the ISP provider discloses the information without a warrant, you think that they should be civilly liable for doing so if it turns out that the individual who took that image hadn't committed an offence at that point and maybe wasn't intending to commit an offence? Why should they have civil liability for doing something that surely we can agree is in the public good?

My concern is, what's the greater public good in this situation, the preservation of harm to that young woman or the preservation of the privacy of the individual who has her intimate image?

The Chair: You have two minutes to answer the question.

Mr. David Fraser: Okay. That will be a challenge.

You're comparing apples to oranges in this scenario. They're very, very different situations. You're also asking me to comment on a very specific example when in fact that police officer would have reasonable and probable grounds to go to a judge or a justice of the peace and get a production order that would make that whole question about immunity moot.

Mr. Bob Dechert: I'm going to interrupt you there. Time is of the essence. We all know that with the Internet, at the blink of an eye, that image could be disseminated to millions of people. The police may not have time to go to the judge to get that warrant, but they want to find out where that individual is so that they can go to that individual and say, "Do not send this image anywhere."

Mr. David Fraser: There are judges available by telephone 24/7 in this country. If you believe...unless it's an emergency. Every telecommunications providers will give information when it's clearly identified to be an emergency exigent circumstance—kidnapping, all the imminent threats to life—so if you can convince them of that, that's fine. Absolutely. And they should hand it over.

But everybody does need to think, in terms of their actions, whether they're cooperating with law enforcement or cooperating with somebody else, whether other legal interests are implicated. Certainly the only person who would be suing in that circumstance would be the suspect. Are they likely to sue? That's probably part of the calculus they would make in deciding that, and that's probably part of the calculus that a number of Canadian telcos have made in deciding whether or not they're going to hand over information about their customers without a warrant. Really, somebody who's accused of child pornography is going to have to go to court and sue us: what's the likelihood of that happening? But I don't think we should take that principle and extend it to everybody.

Certainly if the police were to say they were really interested in what reporters are talking to people on the Hill, so they ask every telco to give them all the calling records of every member of Parliament, they can lawfully ask for that, and perhaps the telcos can lawfully hand that over, but should they be absolutely immune from being complicit in that sort of behaviour? I don't think so. So it's a matter of degrees in a lot of these cases.

● (1250)

The Chair: That's your time. You'll have another slot if you want one.

Madam Boivin, from the New Democratic Party, five minutes.

[*Translation*]

Ms. Françoise Boivin: I find Mr. Dechert's questions interesting.

I think people are afraid that there may be a kind of laissez-faire, a free-for-all, because things move very quickly, because information is accessible, because you can use your Z30 in a flash and get access to all kinds of information. At some stage, it may become a bit of a mess because you can now get warrants in ways that are very different from when I started practicing 30 years ago. You can get warrants in any number of ways. Mr. Dechert's concerns, which are leading him to widen the scope of some matters, do not seem very well founded to me.

However, one thing he said got an immediate reaction from me. Clearly, Bill C-13 has been sold to us as a reaction to the tragic events that ended with the deaths of Amanda Todd, Rehtaeh Parsons, Jamie Hubley and so on. The people from the Boys and Girls Clubs of Canada could certainly provide us with a number of tragic cases.

In terms of Bill C-13, the million-dollar question is the one Amanda Todd's mother asked: would Bill C-13 have saved Amanda's life? Her answer was yes because she is an optimist. I would like to be able to say yes too as she did, but we will have the opportunity to talk to her about it again next week.

However, as Mr. Dechert said,

[*English*]

she came forward.

[*Translation*]

In my opinion, government members are making a mistake to think that, if Bill C-13 is passed, young people who find themselves involved in something tragic on the Internet will automatically call the police. Some of them may perhaps think that they will be able to get back the photo that they had sent in return to someone who sent them a cute photo. But that person could be the biggest pedophile on the face of the earth. I think that we are putting too much stock in Bill C-13's ability to do that. I do not think that is going to happen; it will be

[*English*]

business as usual.

[*Translation*]

How will our police forces react in terms of education? Are they going to be patrolling various places? Will there be an Internet police? Will they be looking for things like that? Are they going to do the things that have to be done, as they do when they drive through our neighbourhoods with their patrol cars? Are they going to be patrolling websites too? Just because Bill C-13 has been passed, I am not sure that kids are going to say—

[*English*]

let's call the cops.

[*Translation*]

Mrs. Marlene Deboisbriand: I think you are right. If Bill C-13 is passed, it does not mean that kids will instinctively call the police. Most of them will not even know about it, actually. That is how kids are.

However, I feel guilty answering that way, because if one young person does something to prevent a tragic situation like the ones we have seen, the ones you have mentioned, that is something important to hold onto. That is why, in the brief we submitted, we indicated that we are not opposed to it. You cannot be against it, but, at the same time, we must not tell ourselves that it will be a magic solution that is going to put an end to the situations we are familiar with. Thinking that would be a little much.

[*English*]

Ms. Françoise Boivin: Okay, go for it.

Mr. Fahd Alhattab: In two seconds, I think there would need to be follow-up action to build—

● (1255)

Ms. Françoise Boivin: Education, for instance, or making sure that the—

Mr. Fahd Alhattab: Who's going to let the kids know? I'm a youth worker—I'm at the Boys and Girls Club—and I find out that one of the kids I'm working with is having trouble. If I'm educated about Bill C-13, I'd say, “Okay, let's talk to Mom and Dad about what we're going to do”. If I'm a teacher or a coach, and I hear about it—and we hear sometimes, and we see, and we don't always know what next step to take.

Ms. Françoise Boivin: They don't always know either. Sometimes they feel ashamed, or they're not too sure what they want to do. They feel like they've done something wrong. It might not be so easy.

There will be a need for much more than Bill C-13.

The Chair: Thank you very much.

Our next questioner is Mr. Dechert, for no more than five minutes.

Mr. Casey, there will be about three minutes left, if you want the last question.

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

Mr. Fraser, do you act in your private practice for ISP providers or other Internet-based entities?

Mr. David Fraser: I do.

Mr. Bob Dechert: If the police were to ask one of them in a situation where, say, a young woman had provided an intimate image to someone consensually, but then became concerned, because of other text messages between the two, that the person who had the image might then post it somewhere on the Internet...and she doesn't know who that person is or where they are.

Let's say Rogers is her Internet service provider and you are acting for Rogers. If the police ask Rogers to give up the information that would allow them to find out the identity of the person who has that image, what would you advise your client to do?

Mr. David Fraser: It's always difficult to talk about hypotheticals with only a limited set of facts.

Mr. Bob Dechert: I understand.

Mr. David Fraser: In the scenario you have described, the image is just about to be widely propagated, causing—

Mr. Bob Dechert: She may suspect it is.

Mr. David Fraser: It is believed to be.

It highlights that it is a very difficult situation. Probably civil liability wouldn't be top of mind.

Let's just say it's an anonymous Internet service provider rather than naming any particular names. They probably don't want to be dragged into a scenario where they can't speak for themselves.

Mr. Bob Dechert: They have a contract with their customer. They also have the common law protection of providing information where there's a suspicion that a crime might be about to occur.

Mr. David Fraser: In this scenario—again, I can only speak for myself—I believe there is a real harm attached to the dissemination of these sorts of images. I've seen first-hand the harm that they can do to a young person, and I've seen what they can do to an adult. My inclination would be to provide that information. That would be my impulse. I would know there might be possibly some risk in doing that, but for me, given the severity of what's going on, this is a non-trivial matter, and my inclination would be to hand over that information.

Mr. Bob Dechert: In that circumstance, you would agree that the ISP provider should not bear any civil liability if it turns out that they were incorrect; there was no crime committed or about to be committed.

Mr. David Fraser: I wouldn't grant them immunity.

Mr. Bob Dechert: You wouldn't grant them immunity.

Mr. David Fraser: No. I would say that they acted in good faith and they wouldn't be liable, but I wouldn't grant them immunity.

Mr. Bob Dechert: That would expose them to a lawsuit, would it not?

Mr. David Fraser: Certainly. Walking down the street exposes one to a lawsuit.

There is a difference between not being liable and having immunity. Immunity is a blanket, saying that no matter what you do, nobody can raise an issue.

Mr. Bob Dechert: Are you concerned that some ISP provider might say, "If I might be subject to a lawsuit that would cost my company thousands of dollars"—I'm a lawyer, you're a lawyer, and we all know how much legal advice costs in this country and how much it costs to go to trial—"then unless I'm pretty darned certain that an offence is about to happen and a great harm could occur, I'm not going to give up the information. I'm going to require the police to get a warrant." In that decision, in that blink of time before a police officer could get a warrant, it's possible that image could be posted and harm could be done to that individual.

Would you agree with that?

Mr. David Fraser: Certainly at any moment there are going to be a whole bunch of considerations. But where I'm coming from, and I want to make sure that I'm clear, is that the reason you have the possibility of liability is because somebody else's interest is at stake and somebody else could be harmed. At that decision point, I want for the Internet service provider, whoever they are, to not only be thinking of the cop who is standing there, or who is on the other end of a phone, and the victim, but also to be thinking about their customers.

● (1300)

Mr. Bob Dechert: But they have a contract with the customer, do they not?

The Chair: That's it, Bob—

Mr. David Fraser: Well certainly, and they need to think about that. But this amendment would gut any liability that might exist contractually. So I think proper decisions are made when you have all the different interests in your mind.

The Chair: I appreciate those questions and answers.

Our final questioner, for a couple minutes, is Mr. Casey.

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

I want to go back to you, Mr. Fraser. On Thursday we had the minister and some officials come before the committee. They were either reticent or outright refused to talk about the relationship between Bill S-4 and Bill C-13.

Why should the minister, why should his officials, and why should we care about the relationship between Bill S-4 and Bill C-13?

Mr. David Fraser: The legislation is intimately connected. The three-quarters of this bill that we have in front of us relates to, in most cases, telecommunication service providers handing over information to the police and the circumstances under which the police can request it and demand it, and then this immunity that actually bestows on those telecommunication providers rights.

That's one-half of a coin, where the other half is regulated by PIPEDA, the Personal Information Protection and Electronic Documents Act. So you have two forces at play, and they are in fact intertwined. So hopefully, when Bill S-4 is being reviewed, they will, in fact.... Although, from what I understand, the minister and the justice officials were not willing to talk about that.

At every part of the PIPEDA review process, which Bill S-4 is the culmination of, Department of Justice lawyers were there acting on behalf of public safety and acting on behalf of others, particularly when it came to the provisions in subsection 7(3), and I would really hate.... Because they interlock together, if you look at this gear in isolation from that gear, you're not going to see how they actually play together, and that needs to be subject to some thorough discussion.

The Chair: Thank you very much.

Thank you to our witnesses today. It was an excellent discussion of Bill C-13 and the issues this committee is facing.

On Thursday of this week, we have the minister and officials coming to talk about the main estimates, and then we'll be back dealing with Bill C-13 likely into the first week, at least, of June, and then we'll be doing clause-by-clause. So just keep an eye on it. That's the timeframe.

With that, I'll adjourn.