HOUSE OF COMMONS
CHAMBRE DES COMMUNES
CANADA

Standing Committee on Justice and Human Rights

JUST • NUMBER 028 • 2nd SESSION • 41st PARLIAMENT

EVIDENCE

Tuesday, June 3, 2014

Chair

Mr. Mike Wallace

Standing Committee on Justice and Human Rights

Tuesday, June 3, 2014

● (1100)

[*English*]

The Chair (Mr. Mike Wallace (Burlington, CPC)): I'm going to call this meeting to order. We have a few housekeeping items before we get to our guests.

This is meeting number 28 of the Standing Committee on Justice and Human Rights. The meeting is being televised as requested. As a reminder to my friends who are on the cameras behind me, these are fixed shots, so no panning the room. Only those who are individually speaking can be televised.

I have a couple of housekeeping items first of all that I want to deal with before we move to the witnesses.

Let me deal with Thursday first. We have a commitment from Facebook to be here live on Thursday. They have requested that The Internet Association also appear. They were was not on anyone's list; this is Facebook's request. They can appear by video conference only. At present we are in Centre Block, because our meeting today is going to be televised, but you cannot do video conferencing from Centre Block until we get it properly wired. We either have to move to another room or to 1 Wellington to have The Internet Association folks appear by video conference.

This time slot always has the issue of potentially conflicting with votes. I don't think it's happening today. I'm leaving it to committee to discuss whether we stick with the Centre Block and have Facebook here, and say sorry to The Internet Association, or move to either to 1 Wellington or stay here and have The Internet Association by video conference.

Madam Boivin, on that point.

Ms. Françoise Boivin (Gatineau, NDP): On that point I'm a bit torn.

[*Translation*]

Mr. Chair, here is what I would like to know.

Can we agree on the following, if we end up with time allocation votes, regardless of how many? I do not want our meeting to be just 30 minutes long. We are in the Centre Block and we are so close to where the votes are held that we can easily keep working here and extend our meeting.

This is the last day we have to hear from witnesses. So let us try to make the most of it. Otherwise, the prudent thing to do would be to reserve next Tuesday's meeting to meet with the other witnesses we have not heard from.

The committee really wanted to hear from representatives from the Internet Association and from Facebook. I congratulate the clerk for insisting that they were witnesses we wanted to hear from. I appreciate his initiative very much and am very happy with it. But I would not like the testimony from the representatives of those two groups to be short-circuited by the bells, because we have 30 minutes to get into the Chamber area and we would be losing those 30 minutes completely.

My answer as to whether we move or not depends somewhat on your answer.

[*English*]

The Chair: Let me respond to that point first of all.

Obviously, I can't predetermine whether there will be votes or not. If we were in any committee meeting and there were bells, if I had the unanimous consent of the committee to continue, I would continue, but only following the rules of unanimous consent.

If you embark on having conversations with your colleagues for Thursday because of the difficulty we've had getting some of the witnesses here, and Thursday's the day they're appearing—and I do want to thank the clerk for all his work on making that happen—I think you might be able to find some agreement around the table. But I can't do that now, and I can't predetermine that now.

On your other item you mentioned, which I think Mr. Dechert had his hand up for too, we had planned for Tuesday to begin the clause by clause. I know you put a motion forward. You don't have to do that when we're dealing with an item, just so you know for future reference. If it's within the study or the legislation we're dealing with now, you can move anything you want as long as it deals with that particular item.

Based on the letter we got from the privacy commissioners from Ontario, British Columbia, and Alberta.... They didn't ask to appear, but they asked us to have the national Privacy Commissioner, so my suggestion is that we put the first hour of next Tuesday aside and invite that individual to come for that first hour. If we need more hours, as a committee we can decide. If not, we go to the clause by clause.

So for next Tuesday, if I have an agreement, we will invite today the new Canadian Privacy Commissioner to come to talk to his report. And I'll hear from the opposition and from the government on what you want to do on Thursday about the rooms.

Mr. Dechert, and then I'll go to Mr. Casey.

● (1105)

Mr. Bob Dechert (Mississauga—Erindale, CPC): First of all, we're content with the suggestion that the federal Privacy Commissioner appear next Tuesday.

Secondly, with respect to this Thursday, we're content to go a bit into the bells period. We'll be in the Centre Block and therefore very close.

Is the issue with respect to the room on Thursday that you can't do a video conference?

The Chair: We cannot do a video conference in Centre Block. Some year, when they close Centre Block and renovate it, we'll be able to do that.

Mr. Bob Dechert: I find this frustrating. My personal view is that having television taping of the proceedings is very important. It would be good to have it in Centre Block for that reason.

The Chair: We can do television and video conferencing from 1 Wellington. We can do both.

Mr. Bob Dechert: But then you'll have a problem with timing because of the bells.

The Chair: The 30 minutes becomes a lot more important, because it takes 10 to 15 minutes to get there.

Mr. Bob Dechert: Exactly.

The Chair: Mr. Casey, any comment?

Mr. Sean Casey (Charlottetown, Lib.): I think we need to hear from the Internet providers association. I would prefer to take the chance that our meeting will be shortened by votes than completely abandon any possibility of hearing from them. For example, Google isn't coming because they're purportedly being represented by these guys. So this is as close as we'll get to talking with Google. I'd prefer to take the risk of the votes shortening the meeting than to not have the chance to hear from them.

The Chair: Okay.

Based on what I'm hearing, let me make the suggestion that since we seem to have unanimous consent to go into the bells a little bit and we do want to hear from everyone, we go to 1 Wellington so that we can have it televised; we get everybody on the record, or at least get their statements on the record; and we have a question period.

Who knows? We may not have any bells. It's just that with that time slot we want to be sure.

Does that satisfy everyone? We'll have The Internet Association; there will be four witnesses then, and we'll go from there.

Madame Boivin.

Ms. Françoise Boivin: The other suggestion might have been to bring them on Tuesday by video conference to 268 La Promenade with the commissioner, if we have the commissioner's office in the first hour.

The Chair: Right, but the issue is that our friends from Facebook want The Internet Association appearing at the same time.

● (1110)

Ms. Françoise Boivin: Okay.

The Chair: So we'll go with 1 Wellington on Thursday. Let's hope there are no votes.

I think that covers off everything.

Your notice of motion we've looked after. We'll invite the new Privacy Commissioner, who will be fully appointed by Thursday. Hopefully they appear. I will let you know on Thursday if there are any issues.

Thank you, witnesses, for your patience on that. It's an important bill, and we want to make sure that all of the witnesses who have been requested to come and see us do so.

As per our order of reference of Monday, April 28, we are dealing 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 a number of witnesses today. Each group will have ten minutes, and then we will go to a question and answer period.

Without any further ado, we'll start with the Bully Free Community Alliance. We have Ms. Anderson, the co-founder, and Ms. Schinas-Vlasis.

Thank you very much. The floor is yours for ten minutes.

Ms. Basiliki Schinas-Vlasis (Co-Founder, York Region, Bully Free Community Alliance): Facebook, Snapchat, Instagram, Ask.fm, Twitter, Vine, Omegle, Yik Yak, Tinder, Voxer, and Kik are just some of the apps and sites that our youth visit, post on, and download from. They are also the 24-hour accessible apps and sites that subject our children to teasing, taunting, torment, and threats, from which the only escape for some has been death.

Good morning, Mr. Chair. My name is Bessie Vlasis. My colleague Gwyneth Anderson and I are co-founders of the Bully Free Community Alliance, a grassroots not-for-profit organization located in York Region, Ontario.

Thank you for inviting us here today. We are honoured to have a voice and to be part of the conversation about Bill C-13.

The Bully Free Community Alliance's mission and vision is to build and sustain positive communities. Our work began over seven years ago when our children became victims of bullying. We witnessed our young, vibrant, intelligent, and happy children withdraw and become physically sick, anxious, and scared. We felt helpless. We searched desperately for support and found ourselves having to navigate the effects of bullying on our own. We knew that pointing fingers and laying blame would accomplish nothing productive, so our research began and our organization developed.

Our organization collaborates with many stakeholders within the York Region community.

We have partnered for the past four years with the York Region District School Board. Due to our long-standing relationship, we sit on their Caring and Safe Schools Committee and are members of their newly formed Cyber Bullying Task Force.

We are contributors to the Ontario Ministry of Education's "Parent Tool Kit", which has just been launched. We are members of the York Region Bullying Prevention Partnership, comprising the York Regional Police, both Catholic and public school boards, Addiction Services of York Region, Character Community, and Children's Mental Health, to name a few. We work with the Toronto Argonauts Foundation's Huddle Up Bullying prevention program, as well as the Canadian Centre for Abuse Awareness. We work directly with the York Regional Police and the Town of Newmarket, including the Newmarket Recreation Youth Centre, where we currently are implementing positive programs and initiatives for youth and their families.

As we discovered early on in our journey, there is very little help or support for victims of bullying and their parents. Often, schools are ill-equipped and lack the knowledge, support, and information necessary to successfully address the problem in an effective manner, particularly in cases of cyberbullying.

Cyberbullying poses significant challenges. It has no boundaries and no limits. It can only be addressed with efforts that parallel its limitless nature. To effect positive change, we must work together. Our efforts must span communities and provincial borders. We must identify the root of the problem, where we are going wrong as parents and as a society, and how we can make it better.

Ms. Gwyneth Anderson (Co-Founder, York Region, Bully Free Community Alliance): We need a culture shift. It's a huge undertaking, but that should not discourage the effort; for it is not a child's privilege to feel safe and welcomed at home, in school, and in their community, but their right, a very basic right.

When children start taking their own lives and mental health issues are at a national high, the adults in this room need to pay attention and we need to take action.

For all of its positive attributes, technology is being used to inflict harm and to socially victimize. Our youth have no safe place to go. It is easy to say to a teenager, "Just turn it off", "Don't look at it", or "Don't read it", but their reality is very much tied to what they see and hear on the Internet and social media.

The number of likes they get on Instagram or the retweets on Twitter are a large part of how they socialize today and where they draw their sense of belonging.

We cannot trivialize the reality that our children live and deal with on a daily basis. The Bully Free Community Alliance views bullying as a large puzzle. Countless people hold the pieces to this puzzle: students, parents, teachers, administrators, school boards, community members, agencies, municipalities, provinces, and our federal government. All of the puzzle pieces need to come together to find and implement a solution.

We acknowledge the efforts of our federal government. We view Bill C-13 as one piece of this complex puzzle. We agree that the Criminal Code needs to be updated and changed for police to respond effectively and quickly to cyberbullying. Is Bill C-13 the answer to the critical challenges posed by cyberbullying? We don't think so; not on its own. But Bill C-13 is a positive first step forward.

We are aware of the controversy surrounding the privacy aspect of this bill. Protecting the privacy of Canadians is very important, but when our children press an app or sign on to social media, do they really have privacy?

All of us have an expectation of privacy when we share online; however, when someone ignores that expectation or takes advantage of someone, that right to remain anonymous is lost and our justice system should be allowed to protect us and keep us safe.

The right to remain anonymous cannot take precedence over the basic right to feel safe and protected. Bully Free Community Alliance believes there needs to be a national strategy that follows Bill C-13. It would not be fair to Canadians to say that this is all we are doing to address cyberbullying.

We can't stop here. Bill C-13 must be bolstered by a national strategy. Technology will continue to evolve at a rapid pace and so will new ways to abuse it. We must respond with a sense of urgency to put an end to social victimization. This has become a matter of saving lives. We must initiate steps to cultivate a growing culture of respect and kindness for each other.

This may sound like an unrealistic and impossible undertaking, but let us reflect for a moment. We changed a culture on how we view smoking because it was killing people. We changed a culture on drinking and driving, and how we viewed that because it was killing people. We changed a culture on how we view the environment because people were getting sick and they were dying. We can certainly change a culture on how we treat each other. Canadians deserve nothing less.

Bill C-13, together with a national strategy, is a groundbreaking step. Canada should lead the way and we should set the example.

We will conclude with a quote from Anne Frank:

> How wonderful it is that nobody need wait a single moment before starting to improve the world.

Thank you.

● (1115)

The Chair: Thank you for that presentation from the Bully Free Community Alliance.

Our next presenter is from UNICEF Canada.

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

Mr. Marvin Bernstein (Chief Policy Advisor, UNICEF Canada): Thank you.

UNICEF appreciates the opportunity to present to this committee, so thank you very much.

We see Bill C-13 as one step in the right direction. We certainly commend the work of the Coordinating Committee of Senior Officials Cybercrime Working Group, which delivered its report. Among its important findings, the working group concluded that existing Criminal Code offences generally cover the most serious bullying behaviour and a new specific Criminal Code offence of bullying or cyberbullying isn't required. However, the working group also concluded that there is a gap in the Criminal Code's treatment of the non-consensual distribution of intimate images or "sexting", which can lead to excessive responses, such as the laying of child pornography charges against young people. It therefore recommends that a new criminal offence addressing the non-consensual distribution of intimate images be created, and this bill provides for it.

While the report covers a number of important issues very effectively, we do have some caveats. The report doesn't address the degree of flexibility required when cyberbullies are children or young people. The report seems to be based upon the contemplation that children and young people will always be the victims, and it doesn't consider the unintended implications of removing specific intent and adding an alternative recklessness standard to the constituent elements of the offence.

We are pleased that this bill is before the committee and is receiving further study at this time.

We also would encourage this committee to consider, as I'm sure you will, the important recommendations set out in the Senate committee report "Cyberbullying Hurts: Respect for Rights in the Digital Age". In that report, there was a strong call for a national, well-coordinated anti-bullying strategy with the provinces and territories. One of the manifestations of not having that coordinated strategy is that we see the provinces and territories branching out and introducing anti-bullying legislation of their own. There are some common elements from jurisdiction to jurisdiction, but there are some significant differences and approaches. Some of those perhaps aren't always in keeping with best practices and evidence-based research, so there is a role for the federal government to coordinate more effectively.

We also propose the development of prosecutorial guidelines that would see young people prosecuted only as an option of last resort.

Finally, we recommend in our brief a series of further amendments to the Criminal Code that would provide for the addition of bullying intent as a requirement of the offence; the deletion of a reckless standard from the offence provision; and the amendment to the open-ended length of Internet prohibitions upon conviction. Right now, the way the provision reads it seems to even give effect to a lifetime ban, which would have very serious implications. We are also recommending an exemption for young people from a child pornography conviction for sexting caught by this new offence and for lawful consensual sexting for selfies.

We would support the provisions in Bill C-13 and commend all of the strong work that has gone into developing the bill, limited to cyberbullying and the non-consensual distribution of intimate images, if its provisions were supplemented by the additional Criminal Code amendments we are proposing. These, together with a well-coordinated, multi-pronged federal-provincial-territorial strategy to combat cyberbullying founded on the pillars of prevention, education, child empowerment, and capacity-building, including the appropriate use of legal sanctions, would balance the best interests of all children and young people, whether their experiences are those of actual or potential victims, cyberbullies, or bystanders.

● (1120)

It's important to recognize from our view that children and young people are not just victims but can also be cyberbullies and bystanders, and even when they are victims they can sometimes move into the roles of cyberbullies and bystanders on other occasions. This requires a careful balancing of their rights and best interests when considering the impacts upon all groups of children in these various roles as they migrate from one role to the other. If we are not careful, the bill may end up inadvertently hurting and punishing some of the very children and young people it's seeking to protect.

We appreciate that for the most egregious acts perpetrated by young persons, the relevant provisions of the proposed legislation are more appropriate as a response than the use of child pornography charges. The fact that the proposed legislation would apply to people of all ages rather than unfairly targeting young people as perpetrators is also welcome.

In tandem with any new legislative response to the broader social problem of bullying, UNICEF Canada urges a stronger focus on education and prevention so that young people, be they potential or actual bullies, victims, or bystanders, understand the social, health, and legal consequences of their digital actions for others and for themselves. Children have the ability and resiliency to protect themselves and others and to alter their own behaviour once they are effectively informed about the risks. We should be empowering children at an early age to become good digital citizens and make informed and responsible choices when they use online media.

In the case of children we urge the development of prosecutorial guidelines for any new legislation so that only the most serious cases result in criminal charges against young people. Such guidelines should also encourage the laying of charges for the non-consensual distribution of intimate images under the new Criminal Code offence once proclaimed in force rather than under the more punitive child pornography provisions of the code where young people are charged.

In addition, we recommend the careful analysis and evaluation of both the intended and unintended impacts of this proposed new legislation on children and young people.

In UNICEF's recent report card on child well-being, Canada ranked 21st out of 29 industrialized nations in the incidence of bullying. Canada must examine what other countries with lower rates, such as Italy, Sweden, and Spain, are doing right so we can prevent more pain, more loss, and senseless death.

We know there are a number of different pieces. This is certainly one component. In a recent Canadian Bar Association webinar speaking to the Nova Scotia legislation approach to cyberbullying, it was explained that protection orders can be obtained through an application to a JP or a prevention order can be obtained after a complaint is made to a director of public safety.

It was conveyed to us that in about 250 orders, virtually all of these orders have been applied for or obtained by schools or by parents. This is not a vehicle by and large that young people are actually accessing so there must be some concern about perhaps being subject to further victimization, or perhaps having their parents fined by virtue of the Nova Scotia legislation.

So we need to find responses. This is one mechanism, but this is really after the fact. When we talk about deterrents, and we explain to young people there might be certain consequences, it's important that, in terms of public spots, in terms of profiling some of the implications, the emphasis should really be on prevention and education. We should be talking about responsible behaviour and engaging in constructive and positive interaction with their peers, rather than the punitive side and perhaps attempting to inject the fear or the spectre of criminal sanctions.

Thank you.

● (1125)

The Chair: Thank you to UNICEF Canada.

Next, we have from OpenMedia.ca. It's Mr. Anderson. I understand you're from Vancouver, Mr. Anderson. I hoped we offered you video conferencing based on that conversation before, so you didn't have to make the trip.

Thank you for being here. The floor is yours for 10 minutes.

Mr. Stephen Anderson (Executive Director, OpenMedia.ca): Thanks for having me, and thank you for this opportunity to speak before the committee regarding Bill C-13.

I'm Steve Anderson, the executive director of OpenMedia.ca. We're a community-based organization working to safeguard the open Internet.

As you may know, OpenMedia.ca works with many other groups to lead the Stop Online Spying campaign, which successfully convinced the government to shelve the lawful access legislation, Bill C-30. Nearly 150,000 Canadians took part in that campaign.

Last year we started the Protect Our Privacy coalition, which is the largest pro-privacy coalition in Canadian history, with over 50 organizations from across Canada.

You know you've hit on a common Canadian value when you have groups ranging from the Canadian Taxpayers Federation, the Council of Canadians, to small businesses, to labour unions, all joining forces on this issue of privacy. As it stands, we have a privacy deficit in Canada, and I'm afraid that Bill C-13 will only deepen that deficit.

I believe this privacy deficit is the result of a democratic deficit. If the government, including members of this committee, were listening to the concerns of Canadians, there is no way you would be paving the way for a range of authorities to have increased warrantless access to our sensitive private information.

To help bring the concerns of Canadians to this committee, I have crowd-sourced this presentation for you today. I asked Canadians online what they thought I should say, and I have done my best to incorporate their input into my presentation. I'll reference them from time to time.

I'll confine my presentation to the lawful access portion, as that is where Canadians have expressed the most concern and I think where I personally also have the most concern.

The Canadians I spoke to had three main concerns: first, immunity for activities that victimize innocent Canadians; second, accountability and oversight; and third, data security.

On immunity, which I'll talk about first, Bill C-13 in its current form provides communications companies that hand over sensitive information about innocent Canadians with absolute immunity from criminal and civil liability.

Recent revelations show that the government agencies made 1.2 million requests for customer data from telecom companies in only one year and that companies apparently complied with those voluntary requests most of the time. After learning of this, Canadians have been looking for more safeguards rather than weakening privacy safeguards.

At the moment, an unlimited swath of information can be accessed by a simple phone call to an Internet service provider. Government agencies don't even need to provide a written request, and we are told that some agencies even refuse to put their requests in writing to avoid a paper trail. This extrajudicial practice works, because there is a loophole that allows authorities to obtain voluntary warrantless access to law-abiding Canadians' sensitive information.

The disclosure immunity provided in Bill C-13 will make the privacy loophole even bigger by removing one of the few incentives for telecom companies to safeguard our data from warrantless disclosures.

Canadian citizen, Gord Tomlin, had this to say on the matter via Facebook:

> If 'authorities' need information, they can get a warrant. It's not onerous, it's one of the checks and balances that is supposed to protect our system from abuse.

Danielle had this to say on the OpenMedia.ca website:

> If accessing an individual's private information is not arbitrary but is justifiable, then a warrant can be obtained. Otherwise, it is expected that the law [will] protect us from privacy violations...

There were many more like that.

Providing telecom companies who engage in extrajudicial disclosure of Canadians' sensitive information is encouraging moral hazard. It's encouraging reckless and irresponsible behaviour.

I'll now move on to accountability and oversight.

Canadians find it troubling that Bill C-13 makes little effort to keep government agencies transparent and accountable. Most shockingly, there is no requirement that officials notify those innocent Canadians who have had their data stored in government databases. The lack of knowledge and consent by those victimized through surveillance and warrantless disclosure is frustrating to many Canadians.

As one Canadian put it:

> I would like to see a requirement that persons whose data has been accessed, be informed of this fact and that there be a major penalty...if there is a failure to comply with this requirement.

● (1130)

The proposed lowering of the "reason to suspect" threshold for transition data warrants is also of concern to Canadians. We're talking about the collection of data—and let's be clear about this—that can reveal political and religious affiliations, medical conditions, the types of activities we engage in online and offline, and whom we socialize with. This is incredibly invasive stuff.

On the topic of accountability, several people also highlighted the costs associated with these data transfers and that they would have to pay for them, and that it would limit our digital economy.

On data security concerns, many Canadians are concerned with how secure data will be once authorities expand their collection through the measures in Bill C-13.

Given recent breaches at federal offices—the CRA and student loans, for example—many Canadians question if we can trust government authorities to properly protect their data from cyber-criminals and identity thieves.

One person online said: The federal government, and indeed the vague category of 'public officials,' has a poor track record of protecting private information already. It's common occurrence in the Canadian news environment to hear about some government agency or officials losing the confidential information of Canadians such as last March's revelation the government had lost the student loan information of nearly 600,000 Canadians. Broadening the powers of officials to access this information only increases the danger that confidential information will end up in the wrong hands.

Bill C-13 also problematically expands the bureaucrats and agencies that can access our private information, including CSEC and CSIS, which are currently facing their own crisis of accountability, given the recent Snowden disclosures. I fail to see how that is connected to cyberbullying at all.

Bill C-13 does not, in its current form, provide effective measures to increase transparency, accountability, or reporting on warrantless access to private data.

In sum, I recommend that this committee remove the telecom immunity and weakening warrant standards, while adding new reporting and accountability measures to this bill.

I also want to join the growing numbers calling for you to split the bill up so that we can move on the cyberbullying portion, which I think there is growing consensus around, minus some reforms, and have a proper debate on lawful access.

As one person put it, "Any expansion of government powers needs to be linked to a compelling societal need."

The lawful access section is not connected to cyberbullying. I don't think that connection has been made for Canadians in nearly enough detail.

I also think it's worth repeating what Carol Todd, the mother of cyberbullying victim Amanda Todd, told this committee. She said:

> I don't want to see our children victimized again by losing privacy rights. I am troubled by some of these provisions condoning the sharing of the privacy information of Canadians without proper legal process.

I think both those on the front lines of law enforcement and Canadians want authorities to have the tools tailored to bringing a variety of criminals to justice. What this bill does at the moment is unnecessarily combine some of those tools with unpopular mechanisms that encourage mass disclosure of sensitive information.

I implore the committee to consider that just one database, the RCMP's Canadian Police Information Centre, has sensitive data on more than 420,000 Canadians. These people have no criminal record of any kind. Many have their information stored due to simply having suffered a mental health issue.

I'd also consider that a Canadian named Diane is one of more than 200 Canadians who recently came forward to say that their personal or professional lives have been ruined despite never having broken the law. Why? Because information about them has been wrongfully disclosed to third parties—in Diane's case, her employer.

Now consider the fact that in recent years federal government agencies alone have seen over 3,000 breaches of highly sensitive private information of Canadians. Consider also that this has affected an estimated 750,000 people.

In Diane's case, she was the victim of a false accusation, which was withdrawn years ago, yet it continues to affect her career. Diane's response after being victimized by this privacy intrusion and having her professional life unfairly curtailed was, unsurprisingly, disbelief, shock, and anger.

Now imagine that Diane was your family member or someone you know. You don't need to put them at risk like this. You can choose to split up the bill and make the necessary reforms whilst dealing with cyberbullying.

Why should Canadian victims be re-victimized by violations to their privacy? Why should those with mental health issues need to live in fear? They don't.

Canadians, including some of the government's biggest supporters, whom I'm working with closely on this matter, are wondering why the government is deepening our privacy deficit when other countries are beginning to rein in surveillance. They're wondering why you're mismanaging our data security.

● (1135)

In closing, as Jesse Kline wrote in the *National Post* last week, "When the Canadian public, parents of victims of cyberbullying, privacy commissioners and former cabinet ministers all voice serious concerns about a bill, it is a sure sign that something is wrong, and the government should listen."

Thank you.

The Chair: Thank you very much for that presentation from OpenMedia.ca.

Our next presenter is from WiredSafety, Ms. Aftab. The floor is yours for 10 minutes.

Dr. Parry Aftab (Executive Director, StopCyberbullying, WiredSafety): Thank you.

Good morning, and thank you very much for inviting me to speak here as a witness today. I wasn't given the option to do it by video conference, but I wouldn't have taken it anyway because I enjoy Ottawa and Canada. I'll tell you a little bit that's not in my prepared notes, but I first fell in love with a Canadian, and I married a Maritimer, so it didn't take long for me to also fall in love with Canada.

I'm an Internet privacy and security lawyer. I run WiredSafety, and we are the oldest and largest Internet safety organization in the world. We are one of five members of Facebook's international Safety Advisory Board. We are the only ones who are uncompensated, to my knowledge.

I also run StopCyberbullying. It's the first non-profit program devoted to cyberbullying also in the world. It's been around for eight years now formally, and much longer informally. We hold summits and bring in young people to help on these issues. Leah Parsons, Glen Canning, and Carol Todd sit on our advisory board at the StopCyberbullying Canada level, as does Sharon Rosenfeldt and Barbara Coloroso. She's been invited, even though she's not a Canadian. Only Canadians can sit on the StopCyberbullying Canada board.

I also have a youth board, and the youth are from all of the provinces in the country, and they provide very knowledgeable input as we look to find ways to improve the safety of other young people. They speak, they do research, and they work with other professionals.

We partner, and we're all unpaid volunteers at WiredSafety, and that includes me. We've been doing this for a very long time. I'm excited to see that Canada is the first country in the world to deal with sextortion, revenge porn, and unauthorized sexting issues.

You also were the first country, through a Supreme Court decision, to recognize that minors may be sharing intimate images consensually with each other. With the couple, if a boy takes it and shares it with a girl voluntarily, or the girl shares it with a boy, or whatever their sexual preferences are, they will not be prosecuted under your strong child pornography laws. It deals with once it starts disseminating.

Notwithstanding the fact that this is a wonderful bill when you're talking about cyberbullying and you're talking about abuse of young people, I think it has some problems. I was the keynote speaker in Nova Scotia when they held their cyberbullying summit, and we held a large summit in Prince Edward Island. When I misspoke before the media, promising that Prince Edward Island was going to do a bigger summit than the one that had been done in Nova Scotia, LinkedIn, Facebook, Google, Microsoft, Barbara Coloroso, Sharon Rosenfeldt, Leah and Glen, all came to little P.E.I. to meet with hundreds of young people and other experts in the room to come up with an action plan for Prince Edward Island. We've done something similar with the first nation community in New Brunswick, and our action plan on cyberbullying will be issued shortly. We're working with the premier there, as well as the premier in P.E.I. We were assisting on the action plan in Nova Scotia from the very beginning. We're working with Alberta, we've worked in Yellowknife. We are all across Canada, as my adopted nation, where I think you can solve the problems of cyberbullying better than we can anywhere else in the world. I do this all over the world.

We had one suicide in Italy because of revenge porn issues and cyberbullying. We're seeing them around the world, but nowhere are we seeing more suicides per capita connected to cyber issues than in Nova Scotia. Little Nova Scotia has had three suicides connected with digital abuse. Rehtaeh was the last, but not the first. And Jenna...Pam Murchison has been dealing with this issue for a long time. We have to focus on it here. This is an island, and this a country known for kindness.

There are old jokes on television when they talk about being kind and people who are courteous in this country, about how you care about each other more than you do in other places. Having two houses in the Maritimes, I agree. I think you do care about each other. I think this is a country of community. We can come up with solutions, a number of people on this panel with me today, and others who you've had testify. We've spoken at UN conferences, we've been on task forces together. You have the talent, you have the expertise, and you have a government that cares about our children, and that's crucial.

The one concern that I have is the voluntary disclosure. It's not that I don't trust the Canadian government with our information. I don't want Rogers, and Telus, and Bell, and all of the other telcos in this country to make a decision about my personal information and who they're going to give it to and whether or not it's authorized.

● (1140)

Giving that immunity to them frustrates me. I carry six cell phone numbers with Rogers. If Rogers won't promise that they're not going to turn over information voluntarily, without a court order, without a subpoena, without a warrant, I'm going to change cell phone companies. If Telus won't promise it, then I won't go to Telus, and if Bell won't promise it, whether it's Bell Canada or Bell Aliant.... Someone who is in the business of providing cell phone and wireless services is going to have to tell me as a customer that they are going to respect the privacy contract, the privacy policy that we've all agreed to. Otherwise I have lost contractual rights with a commercial company that's providing services to me, because of that little immunity clause.

Do I want somebody in a call centre or somebody who's close to someone else, who doesn't understand the standards we need, to have immunity from answering to me? No.

I understand in all likelihood that Bill C-13 will probably pass pretty much the way it is. If it does, I'm going to ask Canadians to vote with their cell phones. I'm going to ask Canadians to turn around and hold their telecom companies responsible for protecting the privacy of their users, and if they don't, then we'll find other ways of communicating with each other. But I think if somebody is going to take a lot of money from me every month for my cell phone, then they're going to have to stick with the promises they made to me.

Canada can have all of the lawful information about us—Canadians or anyone who is in Canada—that they want. I trust the government. I do not trust some low-level customer-service person at a telco to make a decision about my personal information.

I live with death threats. I received the RCMP Child Recovery Award for bringing Amber Alert to Canada on Facebook for the first time in the world. I couldn't go back to Washington for six months—nobody would talk to me—because we did it here.

I live with attacks online from cyberbullies plus. Do I want my personal information exposed in ways I can't control? No. Neither should our children have to do that. When Carol Todd said that she doesn't want anyone to give up their privacy rights in exchange for safety rights—or to do that in Amanda's name—I think that says it all.

I think if we just alter that one provision that gives immunity to the telcos, then I could support this bill. It's not perfect, but it's the best thing on cyberbullying, sexting, and revenge porn that we have seen in the world today. I say that non-stop everywhere I talk and when I reach out to Canadians for help.

You have the head of global policy from Facebook coming here Thursday. You don't have somebody from Facebook Canada; you have the head of global policy from Facebook. That's how seriously they're taking this. I know the clerk has been wonderful in trying to reach out to them, but I should tell you, knowing this from the inside, that they're taking this very seriously as well. They've been looking at it from the beginning.

You have the Internet Alliance. The Internet Alliance is everybody, not just Google or Twitter. Everybody else is in there. You can ask these questions, but don't tell me I have to trust telcos to decide what information they can give away and what they can't, not in the name of protecting our children. We can do it without that, with the help of everyone here.

So I offer my help and assistance while I try to get through all of the papers in all of the places I've lived since I was 18 in order to become a permanent resident of Canada. It takes a while when you're 63. I'm trying to remember. My mother doesn't remember them either. But until then, I am a permanent resident in my heart. I love this country, and I love what you can do, and I don't want anyone sacrificing the rights of Canadians to the benefit of a telco.

Thank you.

● (1145)

The Chair: Thank you very much, WiredSafety, for that presentation.

Our final presenter this morning is Professor Shariff from McGill University.

The floor is yours for 10 minutes.

Prof. Shaheen Shariff (Associate Professor, Faculty of Education and Associate Member Law Faculty, McGill University, As an Individual): Thank you very much.

Thank you for this opportunity to present to your committee.

Parry Aftab is always a hard act to follow. I learned that at the UN.

Voices: Oh, oh!

Prof. Shaheen Shariff: I will try to keep you interested after that.

My submission today relates to three aspects of Bill C-13 that I will address in the following order. I want to discuss the non-consensual distribution provision; the clauses relating to lawful access that have already been mentioned; and clause 12, the hate propaganda provision, which I support.

On the non-consensual distribution provision, Bill C-13 has been widely referred to publicly as legislation that is urgent and essential to reduce cyberbullying. It's been argued, as we've heard, that in the wake of tragic teen suicides, something has to be done to stop the non-consensual distribution of intimate and demeaning sexual images. These online activities amongst teens and university students have surfaced as the most insidious and harmful aspect of this phenomenon. Most often they target teenage girls and young women who are most vulnerable to offline sexual abuse, rape, and other forms of sexual violence, which are videotaped or photographed and distributed online without consent.

Clearly, in light of the suicides and the abuse, there needs to be regulations and consequences. But I have some significant concerns that this non-consensual distribution clause and Bill C-13, when taken together with the lawful access provisions, will miss their mark in reducing cyberbullying and sexting among teens, so I'll outline a number of points.

First of all, the provisions are largely focused on kids who receive contradictory messages from adult society. One thing that we seem to have forgotten when we think about legislating cyber-bulling is the fact that it is adult society that creates the norms of social communication. The norms of social communication have crept towards increased tolerance for sexism, misogyny, rape culture, and homophobia. Popular culture developed by adults, especially online marketing, comedy, and reality shows, place physical appearance, social conformity, objectification of women, sarcasm, and demeaning humour on the highest pedestals of socially accepted behaviour. So what do we expect our kids to do? And then we come down and blame them for copying what adults do in society.

I agree with UNICEF that we need to look at prosecution as a last resort. Even though the non-consensual distribution provision does take away from having to apply child pornography laws, which are designed to protect children against them, there are still questions about the sentencing, how the Youth Criminal Justice Act will be applied, and a range of other concerns.

Children receive confusing messages on the legal boundaries and rape culture, for example. Children confront difficult challenges at both ends. On the one hand, they must prove their strength in a digital and online social network where even friends can demean them publicly and excuse themselves by saying, “Just joking” when under peer pressure they might impulsively react or post comments and photographs they would ignore in different circumstances. Teenage girls are especially vulnerable when they decide to assert their sexuality like female celebrity idols, but end up being publicly humiliated through slut shaming when images sent in trust are distributed without consent. This is not going to be the panacea to addressing some of these issues because it's complex.

One of the areas that we found in our research is that young people confuse fun and have difficulty defining the lines between fun and criminal intent. Youth have difficulty defining the line at which their insults and comments become harmful and illegal, in terms of criminal threats, criminal harassment, sexual harassment, ownership of photographs, and public versus private spaces. It is often a competition about who can post the most absurd insults to entertain friends, and the person who's victimized is actually dehumanized. They totally forget about the person at the end of the vitriol, and thus establishing *mens rea* intent, criminal intent, under the non-consensual clause might be more complex than meets the eye, except in extreme cases.

● (1150)

We need to address the roots of discrimination. It is important to note that the posted content in the forms of abuse both on- and off-line have become more vitriolic, and it is these roots that the law needs to address, not the symptomatic online behaviours by young people. The hate propaganda provisions begin to address this.

There are blurred lines between public and private spaces and content ownership for young people. They told us they have difficulty recognizing the difference between public and private online spaces, the ownership of photographs and videos, because they have grown up immersed in online environments where these lines are blurred. This again could hamper effective application of the non-consensual provisions. These findings suggest that rather than blaming kids for their apparently odd behaviours, we should look at the influence of adult society and adult role models and give them stability and clear boundaries that can guide their moral and social compasses, not harsh laws.

This raises a concern about the current lack of public legal education, because that will have an impact on the implementation of the non-consensual provisions. As far back as the 1980s, Chief Justice Bora Laskin of the Supreme Court of Canada observed an urgent need at that time for public legal education. We are not much further ahead. Implementing this new legislation without adequate public legal knowledge is risky because ignorance often results in reactive and harsher responses.

Our research indicates that there remains significant public ignorance about the differences between positivist laws like the Criminal Code and substantive human rights and constitutional frameworks that provide the balance between free expression, safety, privacy, protection, and regulation. This is the balance the government must strive to aim for. The balance, is repeat, is between free expression, safety, privacy, protection, and regulation.

Without sufficient knowledge about human rights and fundamental constitutional principles of our Canadian Charter of Rights and Freedoms, school administrators, teachers, counsellors, and parents may overreact and be too quick to lay charges or call for charges under these provisions.

We've heard that we need to engage youth in contributing to policy. I'm not sure whether this committee has heard from young people, but it is essential that we give them ownership and agency in contributing to law and policy, as research shows a drop in violence when kids take ownership. The non-consensual distribution clause might be quite confusing for young people who are grappling with defining the lines between flirty fun on Snapchat and harm from non-consensual distribution.

They should have a say in the new law that will affect them so strongly. Without legal literacy they are not likely to understand the ramifications of non-consensual provisions. So we really need to pay attention to the fact that there needs to be legal literacy among adults, among the public, and also among children.

Perpetrators are often victims and, therefore, the non-consensual clause might have the opposite effect if young people who were victims of cyberbullying and react as perpetrators are charged under this law.

As I explained to the Senate Standing Committee on Human Rights a couple of years ago, I am concerned about the impact of reactive legislation on children and youth who are simply testing social boundaries and that includes the perpetrators.

Am I done? I've got one minute, okay. I'm sorry.

On the lawful access provisions—I'm not going to repeat—I have the similar concerns that were raised earlier and I agree with many who testified here that the lawful access provisions should be rejected, or at minimum separated from the remainder of the bill.

● (1155)

If I may suggest, there are many unanswered questions but the committee should pause and ask themselves questions about how well the social online norms and perspectives of young people are understood by prosecutors, judges, law enforcement officers, teachers, and principals. What assumptions about youth will law enforcement, prosecutors, and judges bring to their application of the foregoing sections if they are not well informed about research or about the nuances and complexities of the evolving social norms and societal influences on children and teens? So, along with this legislation, we need to bring in the supports that bring in legal literacy and knowledge for the legal community about how the children are challenged in communicating online.

Thank you.

The Chair: Thank you, Professor. Thank you for that presentation.

Now we go to the question and answer round table that we have. Our first questioner is Madame Boivin from the New Democratic Party.

The floor is yours.

[*Translation*]

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

My thanks to the witnesses who have appeared before us. Your presentations on your respective areas were extremely interesting.

It ties in significantly with what we have been hearing since we began this study. Of course, I would have liked more time to explore the matter more.

Professor Shariff, you began your presentation by talking about clause 12 of the bill, which deals with hate propaganda. You did not really have the time to talk about it fully.

Section 13 of the Canadian Human Rights Act has been repealed. So clause 12 of the bill is the only protection against hate propaganda we in Canada have left. Some categories that were not there before have been added, which is not a bad thing. So I would like to know your opinion in that regard.

Before you begin your answer, I want to thank Mr. Bernstein. UNICEF Canada did an extraordinary job on the brief you presented and the recommendations you have provided us with.

[*English*]

I particularly appreciate and I think your colleagues on the panel probably agree with your recommendations for section 162 to maybe put more on the *mens rea*, on the intent, and to clarify this. So it didn't fall on deaf ears, and we'll probably discuss in the committee certain amendments on that aspect.

The other question I have is for Mr. Anderson of OpenMedia on hate crime. I hope I can join you in saying that I trust the government, but if we were able—and here I use a big "if"—to amend the bill to add some safeguards, remove the immunity that seems to bother a lot of people and maybe have some type of

● (1200)

[*Translation*]

…accountability. In other words, we have to force the authorities that have obtained the information to report on it, somewhat like the way it is done with electronic surveillance under the appropriate section of the Criminal Code.

If we could establish those safeguards—

[*English*]

do you think the bill would be more palatable? And how do you rate Bill C-13 versus Bill C-30? The floor is yours.

The Chair: Professor, you have a couple of minutes on the hate crime piece, and then I'll go for a couple of minutes to Mr. Anderson for his response.

[*Translation*]

Prof. Shaheen Shariff: Thank you very much, Mr. Chair.

[*English*]

I wasn't going to say a lot on it other than to say that the provision in Bill C-13 should be accepted because without it, the discriminatory reroutes of cyberbullying that often perpetrate hatred and division due to people's ethic origin, age, sex, mental or physical disability, or religion will continue to be unjustifiably excluded from the protection of federal law.

I have to say at this point that I also support a submission by my colleagues, professors Jane Bailey, Wayne MacKay, and Faye Mishna. It was a written submission, and I don't know if they presented it at this committee. I was supposed to join them. They have noted that it is particularly important in light of the unfortunate repeal of section 13 of the Canadian Human Rights Act last year. This provision is also essential given the gap in the Canadian public's knowledge of substantive human rights. As I mentioned, there is a need for legal literacy, and so I commend the committee—or at least on this aspect.

Ms. Françoise Boivin: The drafters. Thank you.

The Chair: Mr. Anderson, you have a question.

Mr. Stephen Anderson: I think one difference between Bill C-30 and Bill C-13 is that, thankfully, Bill C-30 mandated warrantless disclosure, whereas this bill doesn't mandate it, but it pretty much in practice means the same thing through the immunity clause.

In terms of accountability, I don't see a lot of difference there. There's very little in terms of accountability or oversight that I can see. I don't understand why there isn't any in here. I don't see why we would not add mandating subscriber notifications. I don't understand why we can't all agree that it's a good thing—record keeping of personal information requests so that we actually can look later and see what's happening and have a kind of data-driven process going forward, and a regular release of transparency reports by both government officials and telecom companies.

I would say that while there's been some progress and learning between Bill C-30 and Bill C-13 on the accountability and oversight side, I haven't seen much movement. I'm hoping that there can be some reforms made in that area. I would love to know if someone could explain why we wouldn't do that.

The Chair: Thank you, madam, for those questions and answer.

Our next questioner from the Conservative Party is Mr. Dechert. Mr. Dechert, you're on the floor.

Mr. Bob Dechert: Thank you, Mr. Chair, and thank you to each of our guests for being here today.

Mr. Bernstein, I'd like to start with you. You mentioned your concern about how this legislation could impact young people under the age of 18. Is there anything in this bill that would prohibit or restrict the application of the Youth Criminal Justice Act?

Mr. Marvin Bernstein: No. I think that what we were trying to convey as well is the...

Mr. Bob Dechert: But you would agree that all the protections of the Youth Criminal Justice Act in dealing with persons under the age of 18 continue to apply, whether it's a charge under the non-consensual distribution of intimate images provision or any other provision?

Mr. Marvin Bernstein: Those provisions under the Youth Criminal Justice Act would continue to apply. I think the point that we were trying to emphasize is that there is a way of strengthening some of the provisions in Bill C-13, so that we don't inadvertently catch certain young people or certain individuals for perhaps some careless behaviours where there isn't the—

● (1205)

Mr. Bob Dechert: The standard is recklessness, not carelessness. Correct?

Mr. Marvin Bernstein: Recklessness, but it—

Mr. Bob Dechert: Do you see a distinction between those two terms?

Mr. Marvin Bernstein: Well, I see that the recklessness standard, as we have indicated in our brief, could create certain problems where there isn't the clear intent to bully. We identify a couple of case examples, such as where an individual provides a laptop to a friend and there may be some embedded sexual imagery, perhaps of a girlfriend. There's no intent to bully the girlfriend, and there may have been some caution given to the friend who borrows the laptop about not accessing any of these files and then the friend goes ahead and accesses the files.

Mr. Bob Dechert: In that case where they've been warned not to access those images, but they do anyway and distribute them widely, you don't think there should be any restriction on doing that? You don't think that the distribution of intimate images without the consent provision should apply in that case?

Mr. Marvin Bernstein: I'm saying that in terms of the boyfriend, this is not something that's being done for any revenge or attempt to be punitive towards the girlfriend.

Mr. Bob Dechert: Isn't that reckless, though? I mean are you suggesting that if I borrow somebody's laptop and the owner of the laptop says, “Look, there are some images on there. Don't look at them, don't do anything with them”, but then I do it anyways and I distribute them widely on the Internet, you don't think that I should be responsible for that action?

Mr. Marvin Bernstein: I'm not talking about the recipient. I'm talking about the boyfriend. The boyfriend who is transmitting the images by virtue of a laptop—

Mr. Bob Dechert: But why would he be charged if he's not the one that distributed the image?

Mr. Marvin Bernstein: No, but he disseminating the image to a friend and there could be some sense—

Mr. Bob Dechert: I don't understand. I don't take your point on that.

If you say “There are some images there, don't look at them”, then I assume you've covered yourself off. You're not disseminating them; you've actually told the person not to do anything with that image.

How can you be guilty of disseminating it?

Mr. Marvin Bernstein: You're transmitting the imagery to the friend.

Mr. Bob Dechert: Frankly, sir, I think most authorities, most crown prosecutors, would look beyond that and look to where the real harm is done, where it's distributed widely to other third parties.

I'll move to Ms. Aftab then, if I can.

Ms. Aftab, are you familiar with section 25 of the Criminal Code?

Dr. Parry Aftab: I am not.

Mr. Bob Dechert: Okay.

Section 25 provides—

Dr. Parry Aftab: I'm a U.S. lawyer, so you'll have to forgive me.

Mr. Bob Dechert: Okay, that's fair enough.

I'd encourage you to take a look at it because you're concerned about the immunity provision. Section 25 already provides that, and has for many years. Anyone who cooperates with law enforcement in a lawful investigation of an offence, or a potential offence, is provided immunity.

Are you familiar with the case law under section 25?

Dr. Parry Aftab: I'm not. If I may say though, if 25 indicates—

Mr. Bob Dechert: I think time is short. If you're not—

Dr. Parry Aftab: —that it's a lawful investigation, I think that's the turning point. I don't think that C-13 requires that it's a lawful investigation.

Mr. Bob Dechert: The point here, Ms. Aftab, and you've clearly stated that you're not familiar with the law, is that section 25 and the case law under section 25 already provide that immunity to the telecom providers.

So, to your point about immunity, all this is doing is codifying what is already the law, and so you should probably be familiar with that. You obviously read the contract that you have with Rogers, and other telecom providers. You know that it already allows them... you've already granted, through that contract provision, the right to disclose your basic subscriber information, your name and address, when you entered into that contract.

The Chair: Questions and answers.

Our next question—

Dr. Parry Aftab: Should I respond to that?

The Chair: The time is up. I'm sorry. Maybe in another round of questions you can do it. That's the political way of doing it.

Mr. Casey, the floor is yours.

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

I'm going to give you chance to respond, Ms. Aftab. But just before I do, at the same time that this committee is meeting, the committee on access to information and ethics is meeting. The witness before that committee is the new Privacy Commissioner. The new Privacy Commissioner, while we have been meeting here, has stated his opinion that he feels that this bill should be split. For those of you who were calling for a splitting of the bill, now you have the national Privacy Commissioner sharing your viewpoint.

I may come back to you, Ms. Shariff, and Mr. Anderson, on that point.

Ms. Aftab, there is something that you didn't get a chance to respond to, with regard to Mr. Dechert. Go ahead.

● (1210)

Dr. Parry Aftab: Thank you very much.

I just want to clarify that I'm an expert on cyberbullying; we've been doing it for 19 years. I'm a U.S. Lawyer in New York and New Jersey, and I'm not familiar with all aspects of criminal law here, although I have seen the responses of the Canadian Bar Association and others.

If indeed the existing law says it's part of an existing valid criminal prosecution, that test, from what I've been able to read, is not in C-13. If it were part of a valid criminal process and an investigation, I don't have a problem with existing law, but that change is what concerns me. It's the arbitrariness of what this is.

I'm not a legal expert here, but based upon just what you said, I see that there is a substitive difference between the two.

Maybe I should be taking Shaheen's legal literacy program so that I know a little bit more about this.

It's a concern to me that there doesn't appear to be a standard. That language is not in this bill. If it were, I might be more comfortable with it.

Mr. Sean Casey: Ms. Aftab, Mr. Dechert wasn't being entirely fair with you. There is a reasonableness standard contained in section 25 of the code that is nonexistent in the immunity provision that the government is seeking to bring in. There is a change and it's—

Dr. Parry Aftab: So, there are standards.

Any kind of standards don't exist under C-13.

Mr. Sean Casey: I want to come back to you on your comments with respect to the relationship between the customer and the telephone companies.

When we asked the minister about the non-consensual distribution of customer information without a warrant, he said, essentially there's no role for the government to play, that it's a matter of contract between the customer and the telephone companies.

I have two questions for you.

First, do you agree that this should be purely contractual? Does government have a role to play?

Second, is there not a marketing opportunity here for the telephone companies, for one company to differentiate themselves from another by saying, “Regardless of what the government asks for, regardless of what immunity they give us, we respect your information, and that makes us different from our competitors”?

Your comments....

Dr. Parry Aftab: Yes, I wonder if there's any support that the telcos are responsible for this provision within the law. They're the ones who benefit. I find it unusual that they haven't commented on this themselves. I think that there is a matter of contract, and I checked the Rogers agreement, and it doesn't say they have the ability to turn over my information except under laws that require so.

So this is voluntary. It's not required in the way C-30 had been, so I think there would be a violation. If I enter into a commercial contract with a commercial provider, I don't think the government should be involved in giving one side a way out without giving me a way out of paying for my service or anything else.

Also, I indicated that it's a great marketing opportunity, and I hope if this is indeed televised, that Telus and Rogers and all of the rest are going to understand that, although the discussion of privacy has been very complicated in this bill, and there's lots of media and lots of things going on, I don't know how many normal grassroots Canadians understand some of the things going on.

Perhaps we haven't done a good enough job of explaining it and we get overly complicated, but if you turn to somebody in P.E.I. or Alberta and ask if he or she is going to use a telco that's going to voluntarily give away information without these standards, I think the answer is going to be no. If somebody says, "We'll stick with your contract, even though it's voluntary. We're not going to go down that road," I think they're going to get a lot more customers right now. They'll certainly get me.

The Chair: You have one more minute.

Mr. Sean Casey: I want to take advantage of your American experience. There are two things I want to ask.

First, given what's happened with regards to Edward Snowden, compare the discussion around privacy rights in general in the U.S. to Canada. You heard Mr. Anderson talk about transparency reports. Given your work with Facebook and Google, what can you tell us in terms of best practices, whether they should be voluntary or legislated, with regards to transparency reporting?

● (1215)

Dr. Parry Aftab: Okay. Best practices are absolutely crucial if they're giving away information. Google and Facebook will not voluntarily do any of this because they're going to face liability in the States or someplace else in the world. So I think you have to have accountability, data, and records. It's not a "Gee, bud, would you send this information over?" I think we have to do it the right way, and there needs to be standards, policies, and procedures so that we don't have the situation that we have in the United States.

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

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

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

Mr. Anderson, I was interested in a couple of comments you made in your testimony. We've had several witnesses say, without a basis for it, that you're lowering the standard in order to obtain transmission data. I don't know where this lowering of a standard comes from, because right now under the Criminal Code, subsection 492.2(1), you can obtain a number recorder. You obtain a number recorder on reasonable suspicion.

Now, what you get with transmission data, in my view, is very analogous to what you get on a number recorder. You will get the origin of the e-mail, who sent it, where it came from, who it went to, when it was sent, and the size of the e-mail. You do not obtain information such as the subject line, content of that e-mail, or information as to a person's location. This is not tracking data.

So I don't understand how you suggest that it's a lowering of the standard, first of all. Where do you suggest it's a lowering of a standard that currently exists in the Criminal Code, and which section of the Criminal Code are you suggesting it relates to for lowering the standard?

Mr. Stephen Anderson: I also am not a lawyer, but the legal consensus that I've heard is that it changes the standard from a reason to believe to a reason to suspect.

Mr. Kyle Seeback: So, you've repeated that without any information as to whether or not it's accurate. You've heard that's what's been said.

Mr. Stephen Anderson: I've heard it from legal scholars whom I trust, including Michael Geist, the Canada research chair, so I think that's a legitimate source. Do you not?

The Chair: You don't ask them questions. They ask you questions.

Voices: Oh, oh!

Mr. Kyle Seeback: No, I disagree with him and I pointed out the section to him, as well.

Where this goes from my perspective on people saying this is such an egregious abuse of people's privacy is the following. You'll have a police officer who will have to get internal approval to go to a court to say to a judge that he or she has reasonable suspicion that a crime has occurred or may occur. They go through their internal chain of command to get approval to go to court. They then go to court before a judge and convince the judge of their reasonable suspicion that a crime has occurred or is likely to have occurred, which is, of course, reasonable. The judge then allows them to obtain transmission data. Somehow that internal approval plus judicial approval equals abuse. I'm not good at math, but to me that seems to be an equation that does not add up, because there are enormous safeguards in that process.

Mr. Stephen Anderson: Well, you should check it again, because they're changing the standard from a reason to believe to a reason to suspect.

Mr. Kyle Seeback: They aren't.

Mr. Stephen Anderson: I think they are, and again, many scholars have come before you to say that. I think that change does weaken the threshold, and I think that right now, Canadians, including in your riding for sure, are looking for more safeguards, not fewer.

The Chair: You have two minutes.

Mr. Kyle Seeback: I think we're going to go back and forth and disagree on that.

I don't think that a police officer is going to go on a fishing expedition to the extent of going through their chain of command to convince their superior that they need to take their limited resources to go to court and take the time to convince a judge just to randomly obtain the data of Canadian citizens because they feel like it. That seems to be what's being suggested by people who oppose this section. And for the life of me I can't understand why busy police officers are going to go on those kinds of expeditions.

● (1220)

Mr. Stephen Anderson: You're putting up a straw man there, because I didn't say that. I don't know of many people who did say that. What I said is that it weakens the standard at a time when people are looking for increased standards.

And why are we doing that in this digital age when this information is actually increasingly more powerful? You can connect to profiles more easily than you could a generation ago. So we should be adding more safeguards, more accountability, and more oversight, which I don't see you adding.

Mr. Kyle Seeback: But they're getting this because they think a crime has occurred or is likely to occur.

Mr. Stephen Anderson: Yes, they suspect it. I get that. I understand.

Mr. Kyle Seeback: And they have to convince a judge that they suspect a crime has occurred or is likely to occur, and to you—

Mr. Stephen Anderson: Yes, so why weaken that?

Mr. Kyle Seeback: —that leads to potential for abuse, a violation of people's privacy.

The Chair: You have 15 seconds if you'd like to answer.

Mr. Stephen Anderson: I do. I think that weakening the standard is taking us in the wrong direction when this information has become more and more powerful in terms of what it reveals about our private lives. And not notifying people who are innocent in these cases seems to be really irresponsible.

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

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

The floor is yours.

[*Translation*]

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

I would like to answer Mr. Seeback's question.

This bill proposes two systems. On the one hand, we have the warrant system, but on the other hand, we are opening the door to a multitude of requests that government agencies could make. We are also allowing public intervenors, distributing the list of people, to have access to the information. Basically, we are creating another system where there is no warrant, no judicial oversight, no obligation to be accountable and no transparency at all.

Mr. Anderson, what do you think about this second system that the bill seeks to create and that clearly requires no transparency? What do you think about the fact that it would be allowing more people to have access to that personal information with no warrant and no transparency?

[*English*]

Mr. Stephen Anderson: I think it's hugely problematic that we're giving more powers, we're extending access to people's private information, to CSIS and CSEC, for example. Right now those agencies have a bit of a crisis of legitimacy; they're in a PR overdrive because of the Snowden revelations. And I think it's appalling that we would actually increase their power at all, especially without accountability and oversight, at this time. We should actually be reviewing what they're doing. That's what we should be doing right now.

So again, it's taking this government backwards.

I would just like to quickly address an earlier point. Someone said that the immunity issue hadn't changed. What has changed, what will be removed, is the obligation to act reasonably and in good faith. I just want to set the record straight on that point, because the fact is that this does weaken Canadians' privacy rights. I've heard from the people in the ridings of all of the Conservatives on this committee, and they're very upset about that. To not pay attention to that, you do at your own peril.

[*Translation*]

Ms. Charmaine Borg: Thank you.

My second question goes to you as well, Mr. Anderson.

Your organization advocates for a free and open Internet. I have looked at a number of your communications in which you make the case strongly that the Internet should remain a free and democratic forum.

Do you have any concerns about the impact that the provisions in Bill C-13 can have on the Internet as a democratic forum?

[*English*]

Mr. Stephen Anderson: Yes, absolutely.

I think that when Canadians are seeing the Snowden revelations and at the same time hearing—not only through this legislation but also Bill S-4—the revelations about CSEC and CSIS.... I think when people hear those stories over and over again, it does limit the discourse and free expression online, and I think that's a problem. I also think it limits our digital economy, because in our digital economy online services are based on trust, and I think Canadians are increasingly losing trust in online services. I would say that in a kind of extra-judicial underhanded way, they're finding out that their data is being handed over to a range of authorities without a warrant. That doesn't make people want to participate in the digital economy. That doesn't make people want to invest in the digital economy. The North American tech sector has been losing billions of dollars since the Snowden revelations, and I think that's an important thing for us to consider here as well.

● (1225)

[*Translation*]

Ms. Charmaine Borg: Thank you.

Mr. Bernstein, my next question is for you.

In your sixth recommendation, you want the maximum length of prohibition on Internet use not to exceed one year. Can you briefly explain why you set that maximum at one year?

[*English*]

Mr. Marvin Bernstein: We were concerned about the implications specifically for young people. There needs to be some kind of ceiling set. The language of the provisions seems to be open-ended. We were concerned, for example, in the case of young people who may be involved in educational pursuits if they can't use the Internet to access information, and do their homework or studies. There are commercial activities. There are young people with disabilities who live in remote communities. One way of staying connected is by using the Internet. There are also situations where employers ask potential employees to complete applications online. It really affects every facet of one's life, so to completely terminate the ability to access the Internet may have disproportionate implications for the life of a young person, or an adult.

I don't know if this was intended, but the way the provision reads, there seems to be the potential for a lifetime ban. No specific statutory ceiling is provided in the legislation—and in distinction to some of my colleagues, I am a Canadian lawyer.

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

The next questioner is Mr. Goguen from the Conservative party.

Mr. Robert Goguen (Moncton—Riverview—Dieppe, CPC): Thank you, Mr. Chair. Thank you to all the witnesses for testifying today. There's certainly a wide swath of opinions that are being shared, and that's helpful, of course, in the examination of this bill.

My question is directed to the Bully Free Alliance and the WiredSafety representatives. The Minister of Justice has indicated that protecting the children, the most vulnerable in Canada, from Internet bullying, from cyberbullying, is a multifaceted problem. It's not only the changes to the Criminal Code, of course, that will accomplish this, it's a much larger puzzle. That's why our government has invested in various, I guess, preventive measures. There are examples of this. For instance, the number of school-based projects to try to prevent bullying.

In addition, through the Get Cyber Safe campaign, the government also supports the Canadian Centre for Child Protection, which operates Cybertip.ca and the Needhelpnow.ca websites, where Canadians can report online sexual exploitation of children and seek help for exploitation resulting from the sharing of sexual images.

So my question to you is, in your opinion, have these investments been useful? Which types of programs have yielded the best results? Is there any particular initiative you would like to highlight to the committee? And last, what other preventive measures do you think the government should invest in?

Don't be shy.

Ms. Gwyneth Anderson: I'm not shy, but I'm not a lawyer, sorry.

Mr. Robert Goguen: No, that's fine.

Ms. Gwyneth Anderson: We brought up the national strategy because we think it should go along with Bill C-13. I think it was Parry who mentioned that different provinces are doing different things.

When we first started, we just started to get involved in our own little elementary school thinking, “Well, we'll just get involved, and we'll just help stop the bullying”. We then realized—it sounds crazy from what we said—it is a culture change.

You can bring programs in. It's like planting seeds, but that's why we suggest that there be a national strategy, so that all provinces and territories are speaking the same language. You have to back it up with education and awareness, because we're just dipping our toe into the digital world. We have a long way to go.

● (1230)

Mr. Robert Goguen: May I stop you there, just for a second—

The Chair: I have to stop everybody. The bells are actually ringing, I don't know why.

It is 12:30, the bells are ringing, so we are required to go to vote. It's a 30-minute bell, so we have to vote at 1 o'clock. Unless I get unanimous consent to continue, which I don't like doing from this distance, we will have to call it a day.

Thank you to our witnesses for coming. We all got on the record. We didn't get as many questions as we would have liked, but we'll be voting at one, so we won't be back in time to continue. Thank you very much for your time.

We will be continuing this process at 1 Wellington on Thursday.

The meeting is adjourned.