HOUSE OF COMMONS
CHAMBRE DES COMMUNES
CANADA

Standing Committee on Justice and Human Rights

JUST • NUMBER 029 • 2nd SESSION • 41st PARLIAMENT

EVIDENCE

Thursday, June 5, 2014

Chair

Mr. Mike Wallace

Standing Committee on Justice and Human Rights

Thursday, June 5, 2014

● (1105)

[*English*]

The Chair (Mr. Mike Wallace (Burlington, CPC)): I'm going to call the 29th meeting of the Standing Committee on Justice and Human Rights to order. We are televised.

Per the orders of the day from Monday, April 28, 2014, we are continuing our study of Bill C-13, An Act to amend the Criminal Code, the Canada Evidence Act, the Competition Act and the Mutual Legal Assistance in Criminal Matters Act.

We have a number of guests here this morning. I want to apologize to them in advance: we are sorry that we were a bit late starting, but we were voting.

I will remind the committee that we had a discussion about votes last time, so that we will be able to accommodate both television and video conferencing. We will go a few minutes into the bells. Based on the lecture we just got from the Speaker's chair, we're not going to go too far into bells, but we'll go a little way.

With that, I want to thank our guests.

To save some time, I will go right to our witnesses.

Our first witness is Mr. Kempton from the Anti-Bullying Initiative.

You have 10 minutes, sir. The floor is yours.

Mr. Roy Kempton (Co-ordinator, Anti-Bullying Initiative): Thank you, Mr. Chairman, and members of the committee. Thank you for the opportunity to speak to you today on Bill C-13 and to share with you what my family has experienced over the past five years as a consequence of bullying.

My name is Roy Kempton, and I live east of Cobourg in Northumberland County. In January 2008, I retired after 41 years as a professional engineer and looked forward to my golden years with my poetry and golf.

Seven months into my retirement, my granddaughter, Abigayle Kempton, hung herself in the backyard of her home on Harwood Road, Baltimore, Ontario, two weeks after her 14th birthday. I still feel the chill of that telephone call. Losing my only granddaughter, I lost the focus of a special love that this grandfather and granddaughter shared, and a common passion for writing. Imagine, then, what her parents felt—the emptiness, the second-guessing

Like any family faced with such a traumatic event, we struggled with emotions. We learned from her final letter she had been bullied both verbally and online, and in her words “wanted peace and to be free of the hurting.” She never spoke much about being bullied. We misinterpreted her mood swings as the trials and tribulations of a growing teenager. Knowing now the pain that bullying caused, we are proud that she made the grade 8 honour roll.

She deleted all hurtful messages from her cellphone and her Facebook page. Police told us these could be retrieved. We did not want this. We felt there was nothing to be gained but more pain. We decided to channel our energies on a positive approach, one that would see good things grow from this tragedy. We made our choice in consideration of Abigayle, a sensitive, caring person with a wonderful sense of humour and a hearty laugh.

We learned about the abuse she suffered from friends. Strange to me even yet, those who bullied her admitted to it, leaving a signed note on her grave asking for forgiveness. As one of them, with her mother by her side, spoke to me of her remorse, I realized that there could be victims on both sides of this age-old scourge. She told me that she was responsible for Abi's death. She cried as her mother told me of her suicidal depression and hospitalization. I cried with her and thought, how sad and senseless this all is. She was a child, just like my granddaughter. I did not see a bully, but a sad, pitiful young girl coping with rampant emotions. This was not a time for retribution or justice, or whatever name we want to put on it.

We needed to do something to avoid such a tragedy happening again. We thought of a scholarship in Abi's name at the high school she planned to attend. It became obvious from support of friends and the wider community, we needed to go further. In May 2009, ABI was founded, an anti-bullying initiative using the acronym of her name. She had plans to study animation at college, and one of the characters she came up with is now used to symbolize our program.

Our initiative tries to highlight the tragic consequences of bullying to grade school and high school students. We developed and set up a website and a Facebook page to reach a wider audience. We also publish a newsletter.

Without professional training, but speaking from the heart, we made presentations at grade schools, high schools, churches, local councils and council committees, scout camps, day camps. We met with families in their homes, and dealt one on one with distressed parents and students. We organized rallies to promote awareness. We have been the subject of several local newspaper articles.

● (1110)

This year marks the fifth anniversary of our initiative. At the end of this current school year, we will have presented $15,000 in scholarships to graduating grade 12 students who have shown exceptional leadership in combatting bullying in their schools and the wider community. We also run a grade-school program where we present t-shirts, pins, bracelets, etc. to deserving students selected by school staff. We are currently working with community groups and with school board representatives to have Abi's story introduced to more schools.

In presenting our story we are hoping we can make a difference. We believe that reaching students at an early age is the key to developing better social skills and behaviour. It really begins with family life where respect for others should be taught.

Are we making a difference? Judging by e-mails, letters, and spoken words of encouragement received, the community believes we are. We know that there are groups with programs out there doing tremendous work to nurture kids to live and be taught in a safe environment. We also know that there will always be those who circumvent standards of decent behaviour that may warrant criminal investigation.

As my friend Grahame Woods wrote recently in *Northumberland Today*:

> In the olden days, when I was a kid, the chant de jour in the schoolyard was 'Sticks and stones can break my bones but names will never hurt me.' Oh, how wrong that was. It was a world where communication was by voice, letter, telephone (for some), even morse code. Yes, today we still have the mindless, oral bullying, but the lethal sticks and stones hurtle through the ether at the thoughtless press of Send - irretrievable, wreaking unseen emotional damage until the recipient can take no more.

Be reminded that it is grandparents and parents who put these sticks and stones in the hands of children as mobile devices, Facebook, Twitter, and other social media. Then we scramble to keep our children safe.

Legislation will help but at the end of the day it remains for families to exercise vigilance in a world where we all struggle to keep pace with changing technology. Children should be aware that there are consequences to the misuse of these devices. Regret cannot erase the emotional impact of hurtful words or images sent facelessly at the touch of a button.

I doubt that the events surrounding my granddaughter's death fall under the provisions of Bill C-13. She was bullied by those she once called friends. It was old-fashioned schoolyard torment with a modern technological twist. Notwithstanding, I understand the need for this legislation and believe it can provide protection to those vulnerable to online activity.

Technology can deprive us of peaceful down times. Our love affair with the Internet has unfortunately undermined the very thing we suddenly wish to hold dear when sadly, in some cases, it is often too late. At fourteen, I could escape to a long laneway with high hedges leading to my farmhouse home on a hill surrounded by trees, with no telephone or mailbox. That kind of privacy was from another world, one we can only imagine now.

I hope my presentation today reflects the spirit Abi exhibited in her short but beautiful life. In an imperfect world, if she had dreams of perfection, it surely would have been to be accepted and respected as she was, with flaws and faults we all have. Respect for others is the core of what this initiative is about. It is what this child taught us. It is what we should teach our children.

Thank you.

● (1115)

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

Our next presentation is from the Canadian Crime Victim Foundation.

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

Mr. Joseph Wamback (Founder and Chair, Canadian Crime Victim Foundation): Thank you, Mr. Chair, and members of the committee.

I'm pleased to attend this hearing today to give witness and to participate in the finalization of this initiative. I'm grateful to see multi-party political support for this bill. For me, my constituency, and hundreds of thousands of Canadians, Bill C-13 cannot be given royal ascent soon enough.

This is not just about young people, but about all Canadians. Bill C-13 speaks to our core belief that the lives and futures of victims of cyberbullying or electronic criminal activity have value and that we, as Canadians, recognize that value. I don't think anyone on this committee has underestimated the horrific effects of cyberbullying on Canadians, especially on our young people.

I wish we could legislate good parenting skills, but as we all know, that's impossible. l also believe that Bill C-13 is not the end. It's just the beginning. We must continue to educate our young people about the life- changing effects of Internet bullying and intimidation and, of equal importance, the consequences and sanctions for that behaviour. I'm a firm believer that consequence is the first step towards prevention. Bill C-13 is the start and for it to be effective, this initiative must be transparent and predictable and, most importantly, it must be perceived as such by all Canadians. That is why I believe that the enforcement and logistics of the legislation are of equal importance and I'm pleased to see them detailed so thoroughly in this bill.

I have reviewed them in detail and I am convinced that there will be no infringements on our individual rights to privacy. I do not believe that the police or the state are threatening the existence of my freedom, nor do other Canadians. I have no concerns about preservation or production orders, nor do any of the parents of victims that I have spoken to recently. I believe that the outcry surrounding these invasions of our privacy are by those who have not read or have understood the provisions in Bill C-13—or they're just being intellectually dishonest.

One of my great concerns has always been the loss of faith in our justice system, especially by our young people. Loss of trust in the system and a belief that it is unjust threatens confidence in our courts and has dangerous consequences, including the serious under-reporting of this type of criminal activity. I firmly believe that the introduction of Bill C-13 will introduce those marginalized and isolated by cyberbullying, especially our youth, that we care and that we are prepared to protect them and enforce this legislation. Failure to achieve this will simply undermine its effectiveness and decrease our collective ability to minimize the occurrence of this type of devastating criminal activity.

Bullying or cyberbullying is not just about the distribution of intimate images without a person's consent. Victims also report that it's impossible to escape from the electronic dissemination of hate and cyberbullying, which includes threats, spreading of false rumours, retribution and, more importantly, social outcasting. It is impossible by the very public nature of the Internet. Its effects are life changing and often result in lost futures, which affect us all.

After a detailed review, I have three recommendations for this committee to consider. First, and I'm sure it has been considered, but I could not find any reference to the Youth Criminal Justice Act in the administration of Bill C-13. Since the initiative of this legislation is aimed at young people, I suggest that the Youth Criminal Justice Act also be cross-referenced with the appropriate amendments to that legislation regarding enforcement, investigation, and sanctions.

Second, I believe that to achieve success we need ongoing education about the details and consequences of cyberbullying. This must be continually and routinely introduced and re-introduced and understood by all Canadians, especially young people, so they comprehend the harm and, very importantly, the consequences of cyberbullying. All Canadians, especially our young people, need to be reminded that anonymity on the Internet does not exist and that we need to ensure consequences are available, that they are consistent, that they are predictable, and that they are recognized for this behaviour.

● (1120)

In the aftermath of the assault on my son in 1999, and for years afterwards, my family received e-mails containing death threats, and horrifically disgusting and accusatory messages and posts on blogs and social media sites degrading my family and my efforts to support crime victims and legislative changes to try to make Canada a safer place for our children.

To this day, we are still victims of these events and nothing could be done because the posts and e-mails were always anonymous. These portrayers of violent intent always remained anonymous and their courage to accuse and defame was housed and strengthened by that anonymity.

l have spoken to many children and families who are victims of similar cowardly anonymous attacks via the Internet and the results are always the same. Threats and the spreading false information, rumours, and accusations electronically are more devastating and crippling to the victim than if made in person, just by the very public nature of the Internet. It is no longer one-on-one; it's there for the world to view.

Therefore, I have a third recommendation, which is hopefully again just housekeeping, but I believe is necessary for clarity and, more important, for greater certainty.

Bill C-13, as noted in paragraph 18, refers to sections 371 and 372 of the Canadian Criminal Code, which are offences against the rights of property. This should be expanded to ensure that other offences that contain language related to outdated technologies, such as the telephone and telegraph, be updated as well. With these proposed amendments, these same acts would be punishable when committed using e-mail, text messaging, blogs, or any means of telecommunications and, most important, would allow authorities the same procedural and investigative tools.

These sections include the following: sexual offences; public morals; disorderly conduct, section 181 of the Criminal Code; and offences against the person and reputation, sections 264 and 265 of the Criminal Code.

Cyberbullying or electronically distributed or perpetrated criminal activity exists because it originates from anonymous, malicious individuals, whose identity is very difficult, if not impossible, to track. The reason it exists is because perpetrators believe they are faceless and can never be held accountable and hopefully this will change.

We will never stop electronic crime or cyberbullying, but I believe that this initiative and subsequent education will create awareness of the effects of online crime and alert our young people about its devastating affects on their peers.

I also hope that it will impose serious consequences and sanctions on those who use the anonymity of the Internet to intimidate and bully.

Thank you very much for your time.

● (1125)

The Chair: Mr. Wamback, thank you for that presentation.

Our next presenter is from the Canadian Civil Liberties Association, Cara Zwibel.

Ms. Cara Zwibel (Director, Fundamental Freedoms Program, Canadian Civil Liberties Association): Thank you, Mr. Chair.

My name is Cara Zwibel, and I'm a lawyer and program director with the Canadian Civil Liberties Association.

The CCLA is a national, non-profit, non-partisan, and non-governmental organization supported by thousands of Canadians from all walks of life. This year CCLA celebrates 50 years of working to protect and promote the rights and freedoms of individuals across Canada.

In our role as a defender of fundamental rights, including freedom of expression, the right to privacy, and the right to be free from unreasonable state intrusion, I am grateful for the opportunity to appear before the committee and raise some of our concerns about aspects of Bill C-13.

My comments today will be focused on two main areas. The first is the creation of the new offence of the non-consensual distribution of intimate images. We believe this new offence as drafted is overly broad and will open the door to capturing lawful activity in a way that may unreasonably violate freedom of expression.

Second, I want to address the new investigative powers included in the bill. Most of Bill C-13 is dedicated to increasing police investigative powers, and in ways that affect not just investigations related to cyberbullying but investigations of any offence under the code. To the extent that some gaps have been identified in the ability of investigators to deal with online crime, such measures are certainly appropriate. However, in our view, the provisions of Bill C-13 do not strike an appropriate balance between investigative necessity and personal privacy rights. They authorize unreasonable intrusions by the state into the personal lives of Canadians. CCLA cannot support the bill without substantial amendments to the investigative powers provisions.

I'll begin with the new offence of non-consensual distribution of intimate images. In starting on this point, I want to acknowledge that cyberbullying is a concern to many Canadians. Indeed, CCLA shares the view that local, provincial, and federal governments have a role to play in addressing this ongoing challenge. There are certainly real harms and a great deal of embarrassment that may flow from the distribution of intimate images. But the criminal law is a blunt instrument, and using it to address the cyberbullying problem may lead to criminalizing the victims as much as the perpetrators.

At the most basic and fundamental level, this new offence criminalizes expression. Even expression that is hurtful, embarrassing, or deeply offensive is protected by the Canadian Charter of Rights and Freedoms, and may only be limited in a manner that is both reasonable and demonstrably justified in a free and democratic society. Restrictions on expression should be narrowly tailored to achieve their intended goals. The goal in this case is a good one. Our concern is that the offence is not narrowly tailored in a way that achieves it.

In our view, the proposed offence is broadly written and limits freedom of expression in a manner that's unreasonable on a number of counts.

First, the offence does not require malicious intent. In light of the ubiquity of intimate images that are floating around in cyberspace, the absence of a malicious intent requirement means that individuals could be held criminally responsible for posting, sharing, or sending an intimate image that is already out there online, perhaps first posted by the individual depicted, and that depicts someone they don't even know.

Second, the definition of what constitutes an intimate image is too broad, and its use of the reasonable expectation of privacy standard will pose difficult challenges to the courts charged with interpreting and applying the law. The concept of a reasonable expectation of privacy, used to give meaning to the right to be free from unreasonable search and seizure under section 8 of the charter, is a complex one. In the context of the section 8 charter jurisprudence, the concern is with privacy interests that individuals have as against the state. The proposed offence, however, deals more with the expectations of privacy that people have vis-à-vis other individuals and society at large. This concept will be much more difficult to interpret and apply when the images at issue were not created by the accused and could have emanated from any number of sources. I've included a bit more information about this in my written submission to the committee.

Third, the CCLA is concerned about the orders that may be imposed on individuals convicted of the new offence, particularly orders that prohibit the offender from using the Internet or other digital network. Such a condition, which under the current wording of the bill may be imposed without terms to limit its scope or duration, is a draconian one. Prohibiting individuals from accessing the Internet may effectively isolate them from friends and family, significantly hamper their ability to access information and communicate with the world around them, and negatively impact the employment prospects and educational opportunities of an offender. CCLA believes this section must be significantly narrowed. As currently drafted, in our view the new offence casts too wide a net, and the recklessness standard that it employs is much too low for an offence that criminalizes such a broad range of expression.

● (1130)

I'd like to move now to discuss the new investigative powers contained in the bill, as these give rise to a number of very serious concerns, particularly in light of information that has recently emerged about the extent to which government institutions are already requesting and receiving personal information from telecommunication service providers and Internet service providers without prior judicial authorization and without the knowledge or consent of their customers.

We are pleased to see that many of the more intrusive provisions from prior incarnations of lawful access legislation have been dropped. But we remain concerned about several aspects in the bill, and in particular the immunity provision found in proposed subsections 487.0195(1) and (2). This proposed section purports to grant immunity from any criminal or civil liability to any person who preserves data or provides a document to law enforcement when there is no legal prohibition on doing so.

On its face, this provision appears to be redundant. It simply states that an individual will not incur liability for doing something that is not prohibited by law. The minister has made statements indicating that this section does not do anything new and is simply there for greater clarity. I've also followed the committee's hearings on this issue and understand that many committee members continue to believe that this provision is totally innocuous.

I have to take issue with this characterization and want to caution the committee against allowing this provision to go forward. Contrary to the statements that have been made, the immunity provision could have far-reaching implications and is deeply problematic.

In particular, it seeks to exploit some of the confusion and ambiguity around the legality of disclosing personal information to law enforcement without a warrant. It also seeks to take advantage of the ambiguity in existing privacy legislation and of the evolving nature of what constitutes a reasonable expectation of privacy in light of increasingly advanced and privacy-invasive technologies.

For example, currently our federal private sector privacy legislation, the Personal Information Protection and Electronic Documents Act or PIPEDA, requires that corporations that collect personal information in the course of their commercial activities not disclose that information without the knowledge and consent of the individual. There are a number of significant exceptions to this rule, many of which are drafted in extremely broad terms and include providing information to government agencies, including law enforcement officials, in a wide variety of circumstances. There remain differing interpretations of the permissible scope of these exceptions, and in light of this ambiguity, corporations may choose to take a more cautious and privacy-protective approach to customer data out of fear of liability.

In our view, that cautious approach is appropriate, given that law enforcement has the expertise and ability necessary to seek out a search warrant. The immunity provision is in our view a blatant attempt to incentivize private corporations to cooperate with law enforcement, even when doing so poses a genuine risk to customer privacy and may not serve any compelling state objective. This provision should be removed from the bill.

A number of the new investigative powers included in Bill C-13 allow for the preservation of data and the production of documents based on the low standard of “reasonable grounds to suspect”. This standard has been found by our courts to be appropriate in contexts in which the reasonable expectation of privacy is relatively low. Bill C-13, however, uses this standard to authorize warrants for transmission and tracking data.

Contrary to statements that have been made that this is akin to phone book information, that is simply not the case. This kind of data can be highly invasive and can provide a detailed and intimate profile of an individual. Many studies have suggested that in some cases, the information that can be gleaned from this kind of data is greater than that gleaned from actually monitoring the content of communications.

I know my time is short. I want to point out also some implications that result from changes to the definition of a tracking device and a transmission recorder.

These definitions have been changed to include software. This means that provisions that authorize the use of a tracking device or transmission recorder effectively allow for the installation of malware. Police are being given the power to remotely hack into computers, mobile devices, or cars in order to track location or record metadata. In some cases, this is done on the lower standard of “reasonable grounds to suspect”, which in our view is inappropriate.

I've addressed the concerns around the change to the definition of public officer in my written submission.

Finally, I want to address concerns around the absence of transparency and accountability mechanisms related to some of the new powers created by Bill C-13.

● (1135)

The new production order powers may result in the disclosure of significant amounts of personal information to law enforcement and a range of others. The bill includes a provision for keeping confidential the existence of these orders throughout the duration, subject to judicial authorization. We understand the need for confidentiality during investigations. The concern is that once an investigation is over, once the investigative integrity no longer requires that this information be kept confidential, there should be proactive disclosure of the fact that an individual's data has been disclosed.

The Chair: That's your time, Ms. Zwibel.

Ms. Cara Zwibel: All right, thank you.

The Chair: There may be questions to which you'll be able to answer further.

Ms. Cara Zwibel: Thank you.

The Chair: Thank you for your presentation.

Our next presenter is from Facebook Inc. Ms. Bickert, the floor is yours.

Ms. Monika Bickert (Head of Policy Management, Facebook Inc.): Good morning. Thank you for inviting me here.

My name is Monika Bickert. I'm the head of global policy management at Facebook. I will be providing my remarks here today in English.

My job at Facebook is all about creating an environment that both encourages people to express themselves and promotes safety and respect. I'm deeply invested in making sure that Facebook is a safe place where people feel comfortable connecting with those they care about. I say this not only as an employee, but also as a mother of two daughters who are growing up in an increasingly connected world.

I came to Facebook after spending more than a decade fighting child exploitation and human trafficking as a federal prosecutor in the United States and as a legal adviser to foreign law enforcement agencies. I share your commitment to keeping people safe online. That's why I feel so proud of the work we are doing at Facebook to give people the ability to connect and to share in a safe and privacy protected way.

We're aware of the complex questions that Bill C-13 raise about cyberbullying, law enforcement, access to data, and other challenges. We appreciate the opportunity to share perspectives with you today on our approach to safety and the way that policy-makers, safety advocates, and industry can work together to build safer communities for everyone, both online and offline. We believe it's important to understand the safety tools, programs, and partnerships that we use to address the challenges of cyberbullying.

Facebook's mission is to help give people the power to share and to make the world more open and connected. Over 1.28 billion people across the globe are using Facebook on a regular basis to share information—messages, photos, videos, and status updates—with their friends and family. That includes over 19 million people in Canada. Facebook is committed to retaining the trust of the people who use our service and to providing a safe and secure online experience.

We've developed a comprehensive approach to keeping kids and others safe on Facebook. That includes strong enforcement of our community standards, robust technological solutions and tools, and partnerships with safety groups to educate people about how best to protect themselves and their friends and family online. We continually work to improve our safety program, and we welcome the feedback that we receive from people who use the service, including policy-makers and safety experts.

Our community standards make clear that we have zero tolerance for bullying, harassment, threats, and explicit content like pornography. We impose strict limitations on the display of nudity. We walk a careful line between respecting people's right to share content of personal importance with the need to ensure a safe environment for everyone in our community. We have teams around the world that work 24 hours a day, seven days a week, to respond to reports about content that might violate our community standards. If content does violates our standards, we remove it from the site. We may also take other actions, such as warning or disabling the account of the person who posted the content or, in extreme cases, alerting law enforcement about threats of real-world violence, self-harm, or child exploitation.

We prioritize serious cases, as well as reports of harassment, bullying and other forms of abuse, because we care very much about people feeling safe when they use our platform. We've also deployed technology to block the sharing of child exploitation images on Facebook, including in private groups, or to flag it for immediate review by our safety team.

In collaboration with Microsoft and the U.S.'s National Center for Missing and Exploited Children, we use a technology called PhotoDNA. This allows us to instantaneously identify, remove, and report to the national centre, known abusive images. The national centre then coordinates with law enforcement around the world to take further action.

● (1140)

We've established a safety advisory board composed of internationally recognized safety experts, who provide us with timely seasoned advice on our products and policies. We try to make it as easy as possible for people to take action based on problems they have or that they see when they're on Facebook. Not only do we have report links that are displayed prominently around the site—you can find these report links on every piece of content on Facebook—we've also created a range of innovative tools and controls for teens, parents, and educators to resolve conflict, both in the online and in the off-line worlds. For example, based on research that we've done about how people communicate concerns to each other, we've developed innovative social resolution tools that allow young people to use Facebook to ask authority figures, friends, and family members for help when they're in a situation where they're feeling uncomfortable.

Our social resolution tools also help young people to speak up when they see others being bullied. Because most bullying that happens on Facebook starts and ends off-line, we realize that even with all of the work that we do in this area, it will always be parents, teachers, and other community leaders who will have the best context to understand what's happening and the best ability to intercede where appropriate.

While tools are important for enabling people to take action on behalf of themselves or others, we also believe that we have an important role to play in educating people about our policies, how to use the tools to help themselves and others, and how to have crucial conversations about staying safe online.

However, we cannot do this alone, so we partner with leading organizations that reach youth across Canada. We're proud supporters of the Government of Canada's get cyber safe campaign. We have worked with officials, as well as the Canadian Teachers' Federation, to promote our "Think Before You Share" guide nationwide. This guide, which you can find—it's publicly available—gives young people the tools that they need to share safely and responsibly, as well as advice for what to do when things go wrong.

The Chair: Can I stop you for one second? Thank you very much.

The bells are ringing, but we had a previous agreement from the committee members that we will continue through the bells.

The current presenter has a couple of minutes left, and then we have another presentation for 10 minutes. My suggestions would be that we hear the presentations, go and vote, and then we'll come back to ask questions.

Is that okay with everyone?

Some hon. members: Agreed.

The Chair: Okay.

The floor is still yours, Ms. Bickert.

Ms. Monika Bickert: Thank you.

Again, we cannot do this alone.

In Canada, during Bullying Awareness Week, we partnered with seven Canadian safety organizations, including PREVNet, Kids Help Phone, and MediaSmarts, on the “be bold: stop bullying” campaign. Students across Canada have learned what they can do to stop bullying and have taken a pledge to prevent bullying in their communities.

We appreciate the government's interest in modernizing law enforcement tools to combat bullying and harassment, and we support finding ways to give law enforcement the tools to fight online crime in a way that respects Canadians' right to privacy. As an industry, we have called on governments to ensure that all law enforcement efforts to collect data are consistent with global norms of free expression and privacy, which means they must be rule-bound, narrowly tailored, transparent, and subject to oversight. We believe that these principles are fundamental to the protection of privacy rights.

In closing, I'd like to again thank this committee for the opportunity to speak with you today. All of us at Facebook share in your commitment to keeping Canadians safe online. We appreciate the opportunity to share some steps that we're taking to maintain a safe community, and our ideas for creating a better Internet.

I look forward to your questions after the break.

● (1145)

The Chair: Thank you very much, Ms. Bickert, for your presentation.

Our next presenter, via video conference, from Washington, D.C., is The Internet Association, and we have Mr. Beckerman with us, who is the president.

Sir, I hope you can hear me. The floor is yours for ten minutes.

Mr. Michael Beckerman (President, The Internet Association): Thank you, and I apologize for not being able to join you in person.

My name is Michael Beckerman and I'm the president of the Internet Association, an organization comprising 25 of the world's leading Internet companies. Our members are leaders in the Internet industry, and as an industry they are committed to providing groundbreaking services to help improve the world. The Internet Association is pleased to be able to share our views on Bill C-13, the act protecting Canadians from online crime.

The problem of bullying threatens people's ability to communicate safely and privately and can have significant consequences for the people involved. Whether it happens in a classroom, on the playground, or on a website, the consequences are exactly the same. It is not a problem that affects any one website, one school, or one medium.

It is clear that no one participant in our society can single-handedly solve this age-old problem. Instead, it's a problem that all stakeholders—families, friends, teachers and other community leaders, along with governments and the private sector—must work on to address collaboratively.

For its part, the Internet industry has worked proactively to address concerns about bullying that occurs online, through education campaigns, suicide-prevention efforts, and robust technical solutions to address bullying when it occurs.

A number of Internet companies, including Google, Twitter, Facebook, and Yahoo have partnered with a non-profit called SAVE, to launch *Responding to a Cry for Help: Best Practices for Online Technologies*, which is a guide for other established Internet companies and start-ups that share the best practices of leading tech companies for decreasing suicide risk among users.

Additionally, our members work closely with groups like the Canadian Centre for Child Protection, MediaSmarts, and others to develop targeted public education campaigns on digital literacy, [*Inaudible—Editor*] online habits, and anti-bullying resources. These efforts are key to stopping bullying before it begins.

A number of our member companies also partner with the Family Online Safety Institute, a global organization, and sponsor their “A Platform for Good”, which is designed to help parents and teachers along with teens to connect, share, and do good online, with the goal of improving online safety for all.

In terms of innovative online tools, our members have robust mechanisms to report abuse when it occurs, including easy-to-report abuse buttons and links that are tied to user-generated content. Our companies also have automated systems, as well as teams of people around the world who review, take down immediately, and respond to content that doesn't meet very strict terms of service and community guidelines.

Although there is no single solution to address the problem of online or offline bullying, we are proud of our members' leadership in bringing new ideas, new resources, and new technology to the table to help our community move forward on this important issue.

The Internet Association members understand that maintaining a safe society requires the involvement of law enforcement. Our members support law enforcement's important mission to maintain people's safety and security, but at the same time we recognize that people choose to use Internet-based services to store some of their most personal and private information. To that end, we believe that law enforcement should be subject to a heightened standard, such as the obligation to obtain a judicial warrant based on appropriate criteria, before obtaining access to people's content, whether that access occurs in cyberspace or the physical space.

Our members are committed to upholding their obligations to coordinate with legitimate law-enforcement investigations, and even go beyond those obligations by building positive relationships with law enforcement, working closely with them in appropriate circumstances. But we do not believe that promoting public safety requires a government to lower its standard for gaining access to people's private communications. Indeed, the public trust requires that we hold ourselves and our officials to the highest standards in this important area.

One of the most important tools used by our members to earn public trust is transparency. A number of our member companies publish the number and types of inquiries they receive from governments around the world. We continue to believe government should be as transparent as possible about the requests they make of companies like Google, Twitter, Facebook, and others, and companies should be able to tell people when their information is being collected by the government, both individually in appropriate circumstances, and in the aggregate.

We are concerned that language in Bill C-13 moves us in the opposite direction. Specifically, subsection 487.019(1) would allow a judge to prohibit persons from disclosing the existence of some or all of the contents of the demand order that they preserve or produce people's private information.

● (1150)

While we recognize there may be limited cases where this kind of a disclosure would create a threat to public safety, this provision of Bill C-13 goes so far as to potentially enable the government to prohibit companies from disclosing even the existence of the demands by government authorities for data, including the number of such demands and whether information was handed over.

Our members publish this type of information because they believe that people should be able to understand the nature and extent of information their government is seeking about them. These reports help give people greater confidence in their governments, that they're acting in an appropriate and a restrained way when they request information about users. And it also helps people feel comfortable expressing themselves online.

We urge the committee to consider drafting this and other gag order provisions in Bill C-13 in a way that would, at a minimum, expressly permit companies to report the aggregate number of preservation and production orders they receive. By continuing to prohibit disclosure of the content of these demands and orders in very limited circumstances where the content of a specific order is particularly sensitive due to security concerns, it is possible to enable that transparency without compromising public safety or legitimate investigative efforts.

As others have noted in public commentary, the bill appears to grant the government powers either to forego a warrant when demanding preservation of data or to obtain a warrant based on lower standards than those currently applicable in the off-line world.

Today I'd like to focus in particular on the second part.

With due respect, we urge the committee to consider whether it is appropriate to lower the warrant standard for government access to individuals' content, as is currently contemplated in Bill C-13. As we understand the legislation, law enforcement agencies would only have to demonstrate to a judge that they have reasonable grounds to suspect that someone has committed a crime or will commit a crime to obtain a warrant. We understand that under current law, police officers must satisfy a higher standard of reasonable grounds to believe that a crime has been committed before they can obtain a warrant.

In addition, the legislation appears to permit judges to consider a lower threshold for determining that the evidence resulting from a lawful search will afford evidence respecting the commission of an offence. Instead, they could grant warrants merely if they will assist in investigation. This is widely viewed as a far lower standard.

In the sensitive area of people's private information, particularly in circumstances where they may not know they are under investigation, it is important that we send a clear message to these people that these kinds of investigations will occur only in limited cases where a high bar has been met.

The Internet Association is concerned that lowering the standard in the way proposed by the bill would both erode privacy of individuals who use the Internet and also reduce the confidence in the government's respect to citizens' due process rights. In light of these concerns, we urge the committee to revert to the existing privacy protective standards in the current Criminal Code.

Our members are responsible companies that are committed to ensuring the safety of Canadian citizens online. The Internet industry will continue to innovate and develop cutting-edge technology and tools, and work on programs and partnerships to address cyberbullying and off-line bullying.

We value the committee's attention to this very important issue raised by Bill C-13. We appreciate the opportunity to present our views, and I look forward to answering any questions you may have.

Thank you.

● (1155)

The Chair: Thank you, Mr. Beckerman.

We will now suspend.

I want to let you know that, based on when we get there, I would like to get the committee back at 12:30. If we could see what we could do to get back here for 12:30, that would be great. Then we'll have one round. We'll do the first round. We'll do seven minutes. It will be a seven-minute round for the first round, and that will be the amount of time we have for our questions.

Thank you very much.

We'll suspend. We appreciate your patience while we go vote.

● (1155)

_____ (Pause) _____

● (1235)

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

I want to apologize again to our witnesses and thank them for their patience.

We are back now from the vote. We will not be interrupted again. We are going to do one round, I believe, as I said before, of approximately seven minutes each.

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

[*Translation*]

Ms. Françoise Boivin (Gatineau, NDP): Thank you to the witnesses.

[*English*]

Thank you so much. In case I switch—I go from one language to the other—be prepared to have translation.

Thank you for your testimony, and I'm thinking especially of Mr. Kempton. I'm deeply, deeply sorry for what happened. Your words touched me. We are going to try to find that right balance, while keeping in mind the real people who are affected by the bills that we are working on. That is a promise I'm making.

[*Translation*]

The same applies to you, Mr. Wamback.

[*English*]

Thank you very much for your testimony.

It's rare that we have Facebook here and the Internet Association.

I will address some of my questions to Facebook in a sense, because I heard your testimony on behalf of Facebook. I'm a big fan of Facebook, so don't take what I'm going to say in the wrong way. I'm one of your 18 or 19 million people from Canada.

At the same time, I remember last year when somebody tried to steal my identity. It was like waking up one morning and having people say, "I don't think it's you." Removing it went well, but we have heard some testimony here about it not always being that easy to remove certain things.

You talked at length about all the efforts and the things that Facebook is making.

You didn't talk much about the legislation, though, so I would like to know what Facebook likes about Bill C-13 and whether there's any part you think we should be addressing. I think we had a good explanation of what Facebook is doing to make it safer and so on, but how does that apply to Bill C-13? Is Facebook concerned about Bill C-13? Do you feel that the orders that could come from courts would apply?

The question might also be addressed to Mr. Beckerman, because a lot of you guys are not based in Canada.

How will that legally affect the companies that you represent, Mr. Beckerman, or Facebook?

Ms. Bickert, are you concerned about Bill C-13? You didn't say a word about it.

Mr. Michael Beckerman: I'm happy to jump in first.

The Chair: We're going to start with Ms. Bickert, and then we'll come to you.

Mr. Michael Beckerman: Yes, so first—

The Chair: Mr. Beckerman, we're starting with Ms. Bickert first. Thank you.

Ms. Monika Bickert: Thank you.

We are very much a global company and we have a set of policies that actually apply to people who are using Facebook, wherever they are around the globe. We certainly comply with all laws that apply to us, but because we're such a global platform, we really take a broad approach to thinking about these issues.

In my testimony, I outlined some of the ways we think about this. In terms of protecting people, we want to take a clear stance in our policies. We want to make it very easy for people to report things, and I hope that the process was easy for you when you had a problem on Facebook. I can tell you that if any content is bullying or harassing and it is reported to us, we respond quickly and take that content down.

Ms. Françoise Boivin: Did you hear the testimony of Mr. Canning, the father of Rehtaeh Parsons, one of the kids who, sadly, committed suicide? He said that it was difficult, and he was told that it was not breaching the community rules of Facebook. There were certain images in which you saw the kid being.... She's dead.

● (1240)

[*Translation*]

She had hanged herself. I do not know how to say that in English.

[*English*]

She hanged herself, or something like that. There were pretty horrible images. So when I hear somebody answering from your group that it was not against the community rules of Facebook, how do you respond to that?

Ms. Monika Bickert: I can't of course speak about a specific case, but that type of content, in which somebody is mocking a suicide, definitely violates our standards and would definitely be removed. It's definitely a priority to us, to the point that we prioritize any report about bullying or harassment so that it will be responded to very quickly across the globe.

To your other point, I don't know if it's more appropriate—

The Chair: I'm going to ask him to answer.

Mr. Beckerman, the floors if yours now.

Mr. Michael Beckerman: Thank you. Sorry, there was a little bit of a delay before.

To the point on our companies being responsive to Canadian citizens or being based in the United States, our companies are all global, and they see themselves as representing the communities and the users they serve, both in Canada and around the world.

On these particular issues there have been a number of very sad and horrific cases, and our companies take that very seriously, and they place a very strong priority on protecting the safety and security of users both in Canada and around the world.

I think you should look at our industry as a whole and particularly our member companies, who are all good actors in the space and are working with authorities in Canada and working with teachers' groups and educating students in Canada, that we should be part of the solution and not to view us as a part of the problem.

Ms. Françoise Boivin: Have you been approached by some police force to divulge some information? Perhaps one of your companies, maybe Facebook, was? Have you been approached in certain cases in Canada to make information available to the authorities? And if so, have you told the people their information was under review?

The Chair: We'll start with Mr. Beckerman on the police requests, and then we'll finish with you from Facebook. Thank you very much.

Mr. Michael Beckerman: I can't get into specific examples from specific companies and individual cases, but I can say that our companies all work with local communities and local law enforcement under the law. In particular, they put a lot of time and resources and effort into cases where people's security or lives are at risk. This is a very important part for our companies.

Platforms are only as good as people allow them to be and having security online, so it's really important we do work with law enforcement on these cases.

The Chair: I'm going to let Ms. Bickert answer.

Ms. Monika Bickert: Any time we receive a request for data from any government, we have a process for scrutinizing it in accordance with our terms and applicable laws, and we will provide data when required to do so by law.

We believe very much in being transparent with the people who use Facebook about how their data's being protected, and when it might be provided to law enforcement. For that reason it's laid out very clearly in our terms in something called our data use policy how we might respond and how we scrutinize law enforcement requests. We've also gone a step further, in that we've provided information publicly in a series of government request reports where we tell people that these are the requests we're getting from around the world, and here's how we're responding.

Ms. Françoise Boivin: And on the immunity clause, how important is it for your companies, and what type of immunity clause are you looking forward to?

The Chair: It's the last question.

Ms. Bickert.

Ms. Monika Bickert: We set forth very clearly in our data use policy the circumstances under which we might provide information to a government. Typically that is in a situation where we would receive a government request, and we would apply very strict scrutiny to that request to ensure that it's not overly broad and to ensure that it is compliant with the law.

In rare cases we make clear in our terms, because we care so much about protecting people, that if we believe somebody's life is in danger or in physical harm, then we will provide information to law enforcement authorities as necessary to protect people.

● (1245)

The Chair: Mr. Beckerman, do you want to respond to that?

Mr. Michael Beckerman: I agree with those comments. On the transparency standpoint, our companies all pride themselves in putting out these transparency reports. It's important for people to understand the type of information that is being collected by governments in a way that is responsive to their needs and privacy concerns.

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

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

Mr. Bob Dechert (Mississauga—Erindale, CPC): Thank you, Mr. Chair, and thanks to each of our guests for joining us today.

Mr. Kempton, I want to join Madame Boivin and express my condolences and sympathies to you and your family for the terrible things that happened to your granddaughter.

I can assure you that your presence here today and all the work you've done previously, including the many public speaking engagements that I know you've done, and the scholarship you talked about will help make a difference for young people. We agree with you that education is the primary important thing to do here.

We're looking at a bill that will put in place some criminal provisions to go after the most egregious examples of cyberbullying and to give law enforcement the tools they need to investigate those. But the most important thing is to give all people the understanding of the power and the speed of the Internet and social media so they can take steps to protect themselves and stop these things from happening in the first place.

So I appreciate your being here, and I appreciate your comments.

Mr. Wamback, it's good to see you again. I know you have appeared before the committee many times, and you're becoming quite an expert in criminal law. I appreciate that.

I was struck by something you said, and it was similar to something we heard from Glen Canning, Rehtaeh Parsons' father. You said anonymity does not exist on the Internet.

Can you explain a little more what you mean by that?

Mr. Joseph Wamback: In my experience, not only personally but also with other Canadians, when they are intimidated and bullied, and their lives threatened and false rumours being spread throughout the various media, not just social media, but various individual blogs and e-mail, this is being done and facilitated because of the anonymity that currently exists. Anybody can log on to any of the social media sites using any name they want and any set of credentials they want to create an identity and continue to work through that identity.

The only thing that is available for the police or for the authorities to identify that individual is the URL, the location and the identity of the computer.

That currently is difficult, if not impossible. I have tried for five years to track down the individuals who have been defaming my family and made death threats against us, and I was told every time that it was to no avail, that it was impossible, that they could not do it.

My hopes with this legislation, given that same set of circumstances, is that we would be able to make accountable those individuals who are utilizing that media to intimidate and threaten, and that there could be consequences for it.

Mr. Bob Dechert: I think Mr. Canning made the point that when people join sites like Facebook or other social media sites, they provide a whole lot of their own personal information to those sites. Sometimes those different organizations do different things. Sometimes they use it for advertising purposes, as with Google and other systems, but the only people who don't have that information are the authorities who are trying to investigate a potential crime.

Ms. Bickert, you told me that people have to use their real name on Facebook and that you take some steps to verify that they are using their real name and who they are. Can you tell us a little more about that?

Ms. Monika Bickert: Absolutely.

We have a policy on Facebook that requires people to use their real identity. And we believe this helps people connect with one another because it goes to the heart of who you are. I can also say that we see that it brings about greater accountability.

We've tried to state very clearly in our policies that this is required—so the expectation is out there—and then provide ways for our community to report to us if they see that something is not right and that maybe somebody is not using his or her real name. When we see those circumstances, we will investigate that profile to ensure that the person is representing himself, and if not, we would remove that profile.

● (1250)

Mr. Bob Dechert: Thank you for that.

I want to point out that Facebook is doing a very good job with these resolution tools and other tools to prevent bullying from happening on Facebook, and taking down questionable content in a proactive way. I think it's showing good corporate citizenship in doing so. I very much appreciate that.

Ms. Monika Bickert: Thank you.

Mr. Bob Dechert: Mr. Wamback, you mentioned the Youth Criminal Justice Act, and I want to assure you that nothing in Bill C-13 detracts in any way from the application of the Youth Criminal Justice Act.

Mr. Joseph Wamback: Thank you.

My concern was that there was no cross-reference to it—and my point was strictly a housekeeping one, as I'm a bit of a fanatic with respect to that—and I wanted to make sure that those provisions would apply equally across all the other sections within the Criminal Code.

Mr. Bob Dechert: We believe that they do, but we can certainly take a look at that.

Mr. Joseph Wamback: Thank you.

Mr. Bob Dechert: Ms. Zwibel, are you familiar with the report of the Cybercrime Working Group of individuals representing each of the provincial and territorial attorneys general?

Ms. Cara Zwibel: I am.

Mr. Bob Dechert: And you're familiar with the recommendations in that report?

Ms. Cara Zwibel: Yes.

Mr. Bob Dechert: Are there any recommendations you disagree with?

Ms. Cara Zwibel: It's been a while since I looked at it, but I know that one of the recommendations resulted in the proposal to create this new offence of the non-consensual distribution of intimate images. As I said earlier, it's not the creation of that offence in itself that's problematic, but in our view, the way it's been drafted.

I think the recommendations also did speak to increased investigative powers, which are in the bill—

Mr. Bob Dechert: And do you agree with them?

Ms. Cara Zwibel: No. I took issue with a number of them in my presentation earlier. We're concerned about the reasonable suspicion standard for some of the—

Mr. Bob Dechert: So your organization disagrees with the recommendations of the Cybercrime Working Group in that regard?

Ms. Cara Zwibel: Yes, in that regard.

Mr. Bob Dechert: Thank you.

You mentioned the so-called immunity provision in 487.0195. Are you familiar with section 25 of the Criminal Code?

Ms. Cara Zwibel: I am.

Mr. Bob Dechert: It provides some measure of protection for those who cooperate with law enforcement.

Ms. Cara Zwibel: Yes. The wording of section 25—I know that this has come up in other—

Mr. Bob Dechert: Can I ask you one more question? I think it's relevant.

Ms. Cara Zwibel: Sure.

Mr. Bob Dechert: Are you familiar with the case of R. v. Ward and the Ontario Court of Appeal decision by Justice Doherty?

Ms. Cara Zwibel: Yes, I know the case that you're talking about.

Mr. Bob Dechert: Taken together, section 25 and that decision by Justice Doherty in the Ontario Court of Appeal, do you agree that this provide some immunity to Internet service providers and others who are asked by police to voluntarily disclose basic subscriber information such as the name and address of...?

Ms. Cara Zwibel: My answer is that it depends. The basic subscriber information that would be given in exchange, for example, for a listed phone number is the kind of information that you would expect to find in a phone book and that individuals generally expect to be publicly available. When you have a request that's made by law enforcement to an Internet service provider, a telecom company, and the seed of the request is an IP address, an Internet protocol address, then you're asking for subscriber information. In my view, that reveals more than what's publicly available. That reveals the places that you're going on the Internet, the sites that you're visiting.

Mr. Bob Dechert: But not any content, or images, or anything of that nature.

Ms. Cara Zwibel: Not content or images, but if you know the site that someone's been to, you can gather what the content is on that site.

Mr. Bob Dechert: Thank you.

Can I ask you, Ms. Bickert, for your interpretation of what the IP address discloses? If Facebook asks for that information, what do you think you're disclosing to police?

Ms. Monika Bickert: When we provide...?

Mr. Bob Dechert: The subscriber information for an IP address, for example.

Ms. Monika Bickert: We do provide non-content-based information, such as IP addresses, when we get legally sufficient requests from government. Beyond that, I'm not sure I can—

Mr. Bob Dechert: That is covered in your agreement and in the policies that people agree to when they sign on to Facebook?

Ms. Monika Bickert: Absolutely, it's very transparent—

Mr. Bob Dechert: In your opinion, what does the IP address information disclose? Is it just the name and address of the person sending that transmission or is there other information?

Ms. Monika Bickert: We would provide the IP address. How that is used or—

Mr. Bob Dechert: Would they then go to the actual IP address?

Ms. Monika Bickert: I wouldn't have that information.

The Chair: No problem. Thank you very much for those questions and thanks for those answers.

Our final questioner is Mr. Casey from the Liberal Party.

● (1255)

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

Ms. Zwibel, you were asked a question about the relationship between section 25 of the Criminal Code and Bill C-13. You started to rifle through your papers to get an answer and you weren't afforded an opportunity to answer the question. This is your opportunity.

Ms. Cara Zwibel: Thank you.

Section 25 says that if you're required or authorized by law to do something, and you act on reasonable grounds, you're justified in doing that. It's basically a justification defence. It's a little bit different from the blanket civil and criminal immunity that's being proposed in Bill C-13. The provision in Bill C-13 doesn't require the reasonableness, so I think there's an important distinction. I think section 25 is, with respect, a bit of a red herring.

Mr. Sean Casey: I think so, too. Thank you.

Mr. Beckerman, to your knowledge, has your association or any of its members been consulted in the process of developing this legislation?

Mr. Michael Beckerman: Not to my knowledge for the association. I can't speak to all of the individual companies or if they've been consulted on this legislation.

Mr. Sean Casey: Is an immunity against civil and criminal proceedings for voluntarily disclosing information to law authorities in Canada something that your association, or any of its members, was asking for?

Mr. Michael Beckerman: As I mentioned, I can't speak to individual conversations that our companies may have had with the committee when drafting this legislation. To my knowledge, at the association, we haven't been involved in the drafting of the legislation.

Mr. Sean Casey: Does your association count among its members telecommunications companies?

Mr. Michael Beckerman: We do not.

Mr. Sean Casey: This question is for Ms. Bickert, and also for you, Mr. Beckerman.

Each of you talked at some length about transparency reports. I don't know whether you're aware that it's been very difficult to get the type of information, which you voluntarily disclose, from telecommunications companies. I'm talking about the non-consensual distribution of customer information without a warrant.

What can telecommunications companies, and perhaps the government, learn from your practices with respect to these transparency reports?

The Chair: Ms. Bickert, do you want to answer first?

Ms. Monika Bickert: Trust is really the cornerstone of our business. The simple truth is that if people don't trust Facebook, they're not going to use it. For that reason we make clear, both through our policies and our practices, that transparency is paramount to us. That's why we put in place the procedures that we have. That includes not only outlining how data is secured and how it could be provided in response to a lawful government request, but also voluntarily providing transparency reports so that people can understand the scope of the way governments are seeking access to data.

The Chair: Mr. Beckerman.

Mr. Michael Beckerman: Thank you.

I can't speak for telecommunications providers. I can just say that for our industry, transparency and user trust are paramount. Our sites are only as good as the users who interact with them. In our industry, competition is everywhere and competition is really just a click away on the Internet, which our companies are very mindful of. So transparency and accountability to users is incredibly important and it's fundamental to the industry.

Mr. Sean Casey: If the government agreed with you, there would be no reason they couldn't legislate it, or even incorporate it into this bill. I expect you're not a big fan of having government legislate what your practices are, but it seems to me that what each of you is doing represents a best practice that could possibly be legislated.

Would you care to comment on that?

The Chair: We'll start with Mr. Beckerman.

Mr. Michael Beckerman: As I mentioned in my testimony, transparency is incredibly important, particularly the reports that many of our companies do in the aggregate on requests for data from governments. We do have some concerns with the legislation that it could block a number of these transparency reports that we find very important.

● (1300)

The Chair: Ms. Bickert.

Ms. Monika Bickert: We certainly comply with all applicable laws, but we take the approach that we do to transparency because it's important to us and to the people who use our product.

Mr. Sean Casey: Mr. Beckerman, you seem to be suggesting that the legislation stands in the way of telecommunications companies being more transparent. Do I understand you correctly?

Mr. Michael Beckerman: The way I understand the bill is that through judicial oversight, it could block the aggregate disclosure of information requests.

Mr. Sean Casey: Thank you.

Ms. Zwibel, do I understand you correctly to say that Bill C-13 will result in tracking devices, including software, and that it would afford government the power to install malware to track a person? Did you say that?

Ms. Cara Zwibel: I did, and that is my understanding of the change to the definition of a tracking device and a transmission data recorder. I can pull out the sections.

This is something that was recently brought to my attention by some people who are much more technologically savvy than I am. There is a blog post about the change that this represents by a gentleman by the name of Christopher Parsons, who is a post-doctoral fellow at the University of Toronto.

It's my understanding that what this does, in changing the definition.... It used to be that with judicial authorization you could, for example, attach a device to a car if you wanted to track where that car was going. The fact that the definition now includes software and that it could be extended to a device that an individual has with them, means that malware might be installed on a mobile device or a computer or even in the internal computer of a car.

In my view that's a significant change. As I said, I've done my best to understand the technology behind it, but those who know better than I have suggested that this means there is the potential for the surreptitious installation of malware by police.

The Chair: You have one more minute, Mr. Casey.

Mr. Sean Casey: Ms. Zwibel, you're aware that there is presently a piece of legislation before the Senate, Bill S-4, Digital Privacy Act. I think it's been admitted by the minister that there is a link between it and Bill C-13, yet both the minister and his officials were either reticent or outright refused to discuss it.

Why is the link between these two pieces of legislation important?

Ms. Cara Zwibel: The provision in Bill S-4 that has the most relevant link to Bill C-13 is a provision that expands the exceptions in PIPEDA, which I mentioned earlier.

Right now there's an exception, so that a company does not have to seek an individual's consent before disclosing their information to law enforcement or government agencies in certain circumstances. This would expand that to include other organizations that might be requesting information where there's an allegation of breach of contract, for example, copyright claims, and things of that nature.

Really, the problem is that it puts the holder of the information, a private corporation, in the seat of an arbitrator of a contractual dispute or a law enforcement issue, and those are the things that should be done with judicial oversight.

The immunity provision in Bill C-13 obviously plays a big role. In our view. If the provision in Bill S-4 passes, there is an incentive for companies to hand over more information both to law enforcement and to others requesting information. We think the incentive should be going the other way.

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

I want to thank our panel for being here today.

Just so that the committee knows, we have invited the Privacy Commissioner. He just confirmed that he will be here on Tuesday for the first hour. Then we'll be going clause by clause. I know that the Liberal Party has already submitted a few amendments. Please provide the amendments by tomorrow noon, if possible, so that we can look at those and get ready for the clause-by-clause consideration starting next Tuesday afternoon.

We will have one more meeting on this and then we'll be proceeding....Thank you very much for your patience and for being here with us today.

With that, we're adjourned.