

Standing Committee on Justice and Human Rights

JUST • NUMBER 025 • 2nd SESSION • 41st PARLIAMENT

EVIDENCE

Thursday, May 15, 2014

Chair

Mr. Mike Wallace

Standing Committee on Justice and Human Rights

Thursday, May 15, 2014

● (1100)

[English]

The Chair (Mr. Mike Wallace (Burlington, CPC)): We're here at the Standing Committee on Justice and Human Rights, meeting number 25

For the orders of the day, we have the committee business that we weren't able to complete at the last meeting because our guests took up the whole time, which was fine. But we do have the main estimates. We have looked at the mains here as a committee, so what we need to do, and what we'd like to do first, is to deal with them. I want to deal with them in the same way we deal with them in the House, so I will read them out, and we'll do it on division, as is the norm

So if you could just bear with us for a minute guests, we'll be with you in a second.

For the main estimates of 2014, I call the following votes:

CANADIAN HUMAN RIGHTS COMMISSION

Vote 1—Program expenditures......\$19,639,234

(Vote 1 agreed to on division)

CANADIAN HUMAN RIGHTS TRIBUNAL

Vote 1—Program expenditures......\$4,145,232

(Vote 1 agreed to on division)

COMMISSIONER FOR FEDERAL JUDICIAL AFFAIRS

Vote 1—Operating expenditures......\$8,643,425

Vote 5—Canadian Judicial Council—Operating expenditures........\$1,513,611

(Votes 1 and 5 agreed to on division)

COURTS ADMINISTRATION SERVICE

Vote 1-Program expenditures......\$61,260,445

(Vote 1 agreed to on division)

JUSTICE

Vote 1—Operating expenditures.....\$236,861,079

Vote 5—The grants listed in the Estimates and contributions......\$317,485,223

(Votes 1 and 5 agreed to on division)

OFFICE OF THE DIRECTOR OF PUBLIC PROSECUTIONS

Vote 1—Program expenditures......\$149,579,834

(Vote 1 agreed to on division)

SUPREME COURT OF CANADA

Vote 1—Program expenditures......\$22,307,652

(Vote 1 agreed to on division)

The Chair: Shall the chair report vote 1 under the Canadian Human Rights Commission, vote 1 under the Canadian Human Rights Tribunal; votes 1 and 5 under the Commissioner for Federal Judicial Affairs; vote 1 under Courts Administration Service; votes 1 and 5 under Justice; vote 1 under the Office of the Director of Public Prosecutions; and vote 1 under the Supreme Court of Canada to the House?

Some hon. members: Agreed.

An hon, member: On division.

The Chair: I'll report those back, thank you very much.

We have two more quick items.

First, the supplementary estimates (A) were introduced in the House yesterday. There are no supplementary (A)s for this committee, so we won't need to deal with supplementary them, which makes me very sad. Anyway, there aren't any, so we have nothing to do.

Second, we made a commitment that we would try to bundle witnesses—you can see here today that we have the police forces. We have one issue. The people from Facebook cannot make it on the day that we're having other Internet providers here. They're willing to come a week later, so with the permission of the committee, we will put them on another panel. It might not be a full bundle, but we'll have Facebook as an organization.

We do want them here. I would agree with that.

Okay? Thank you very much.

As to the order of reference of Monday, April 28, 2014, 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 witnesses today to talk to us about the bill.

We have the Canadian Association of Chiefs of Police here, with Mr. Jim Chu. From the Ontario Provincial Police we have Carson Pardy. From the Royal Canadian Mounted Police we have Joe Oliver. And there are others here with them, who will introduce themselves. From Halifax by video conference we have Jean-Michel Blais, the chief of police.

Thank you for joining us. Each organization will get 10 minutes to address the committee, and then there will be a question and answer period

My first witness today is from the Canadian Association of Chiefs of Police.

Mr. Chu, the floor is yours.

Chief Jim Chu (President, Chief Constable, Vancouver City Police Department, Canadian Association of Chiefs of Police): Good morning, Mr. Chair and honourable members.

I'm pleased to be here as president of the Canadian Association of Chiefs of Police. I'm also the chief constable of the Vancouver Police Department.

As mentioned, we're the bundle known as the CACP. We represent over 90% of the Canadian police community, including federal, first nations, provincial, regional, and municipal police agencies. We're really pleased to be able to present information first-hand.

First of all let me say this. The CACP fully supports Bill C-13. Let me get right to the concerns we're seeing on the front lines of Canadian communities every day. The proliferation of crime has moved to the online environment.

Traditional crimes, like criminal harassment, threatening, kidnapping, fraud, a decade ago would have been conveyed with a letter or something through the mail, or perhaps a voicemail. Now, as we know, the vast majority of those crimes are perpetrated online, through text messages, e-mails, through Facebook postings, through revenge websites, through message boards like ask.fm, Kik, or many more websites that exist in cyberspace.

I should also note that a lot of these websites that are used by young and old are based overseas in countries like Latvia or other places in Eastern Europe.

Let me focus right in on young people today. I have this information from our school liaison officers who work in the high schools and elementary schools in Vancouver. Their experiences are similar to what's experienced across Canada.

The amount of online bullying, threatening, sextortion, harassment, and stalking online is more prevalent than ever. Why is that? I look around the room and think that some of us in our youth had to meet the bully face to face in the playground or in the hallways. Schools could deal with that by either moving you or moving the bully, and that would end it, whereas now in the online world it doesn't end. It's 24/7. You go home at night or you go out on the weekend, the bully gets kicked out of school, and it can still continue.

Moreover, many more people can be a bullies. Before, you had to be doing it face to face, whereas now those bullies are emboldened by the anonymity of the Internet, so there are more people doing it. In fact, there are more people being predators out there as well.

Probably all of you, because I know you're in political life, have seen the venomous, abusive comments that are one of the dark sides of social media. As adults, and as people in public life, we're used to coping with it. But think of young people. When they experience something like that it's extremely traumatic. It's frightening, and it progresses to the point where the victims causes harm to themselves because they're so upset and traumatized by what's happened to them.

These are the young people who don't have any safe haven.

Also, if something is posted online can mean that it's out there forever. At least with a written note you can destroy it, put it in the garbage. A written note is passed among just a few people. Those are all who see it. Now, online means the world can see it.

To combat this problem, the police need modernized tools. We need to intervene quickly to stop it from becoming worse.

For a lot of young people, when we're intervening it's not going to result in charges. Give us the tools to help more of these victims, and when we do have a victim, help us to stop the bullying and the harassment early, and stop it from becoming worse, because the worse it gets, the more serious it becomes. Then, of course, it is very traumatic for the victim.

It could lead to criminal charges. In the majority of cases we handle right now, we just resolve at the school level and it doesn't result in criminal charges.

But remember that some of those young people who perpetrate cyberbullying are making bad decisions, whether it's from bad influences in their life.... Again, we want to stop them so that they don't progress to doing something stupid that causes harm to someone else, and they will have to live with that for the rest of their life. Or, if they're taken through the criminal justice system, again, those will be consequences they will have to live with for the rest of their life.

Help us to intervene early.

Of course, we are also engaged in education and we partner with our schools. In Vancouver, especially, we have multilingual brochures because the schools have a struggle to keep up with the technology. Many parents have an even harder time, especially if they are new to Canada, to be able to monitor what their kids are doing, and to put in place protective measures so their kids are acting responsibly.

Let me say this. Canadians believe in privacy rights, and so do the police. We have seen that Bill C-13 does not create any ability for the police to compel the release of information that does not go before a judicial authority. That's a very important point. But it helps us get certain information quickly, for example, the routing of Internet traffic so that we can determine who sent a threatening message.

• (1105)

Sometimes that's going to be a dead end. So give us the tools that help rule out those dead ends. For example, we may go through a telco and get information that tells us something originated in a Wi-Fi café. Hopefully we can resolve that and determine that in a matter of hours, not several days, which can be the case right now.

Let me conclude by talking about the concerns of the public and the misinformation that's been spread. I don't know if it's inadvertent or deliberate, but I'll give you three examples of incidents that I've seen recently in the social the news media.

This is a picture of a police officer listening to the phone call of a young girl. There's also another variation of this picture. This same police officer, the actor, is standing over somebody as they surf the Internet. Today, to monitor phone calls in real time we need a wiretap warrant. Those are very hard to get under part VI of the Criminal Code. Those wiretap warrants take 500 to 1,000 pages. They can take weeks to write. My point is that Bill C-13 doesn't change that. We cannot do that. As for monitoring the surfing habits of Canadians, I asked our officers in the Vancouver police department and they said they'd never had part VI approval for an IP address. It rarely happens.

Let me point out another news story that kind of gave me cause for reflection. It's titled, "How federal bill C-13 could give CSIS agents—or even Rob Ford", referring to the mayor of Toronto—"access to your personal online data". In the Criminal Code, there is some ancient wording that says a mayor is a peace officer, and I suppose a mayor could exercise their powers and make arrests on the streets of their communities, although I've never heard of one doing that. But I would be flabbergasted if a mayor wanted to write a production order, show up at a telco and say, "Give me private data". It's not going to happen. So putting Rob Ford's name in this headline I think unnecessarily alarms Canadians and is unfair to legislation that's coming forward.

This last opinion article starts with this, and it's from a Halifax newspaper.

Picture this: You arrive home tonight to discover that your friendly neighbour-hood police officer is going through your papers and your computer files, making notes on your private information — without a warrant.

If you picture that, it's concerning. Can that happen? First of all, there's no provision for us to do that today without a warrant to search a home, to search a private computer. Warrants have to be obtained from judges with reasonable grounds to believe it's a very high standard. But the writer equates that to Bill C-13, saying that now it's warrantless access to all the Canadians' private information.

In closing, I know Canadians are concerned about their private information. This bill does not allow the police, nor do we want, to go through the private information of Canadians without the proper judicial authorizations. Please give us the tools to help stop people from being victimized. And for those people who have been already victimized, give us the tools to help them not be retraumatized, because the investigation takes days and weeks as a result of our cumbersome processes to get the necessary information to identify the perpetrators.

I will now turn it over to my colleague—

● (1110)

The Chair: That's okay, thank you very much, Mr. Chu.

Our next witness is Mr. Pardy from the OPP.

Mr. Carson Pardy (Director of Operation, East Region, Ontario Provincial Police): Good morning, Mr. Chair, and members.

It's a pleasure to be here today, and on behalf of our new Commissioner Vince Hawkes, it is my pleasure to be here to represent the almost 6,200 uniformed and 2,800 civilian members of the Ontario Provincial Police. Joining me today is Staff Sergeant Carole Matthews, manager of the OPP technological crime unit, who can address some specifics regarding the investigation of technology-based crime on a number of levels.

We appreciate your interest and welcome the opportunity to speak to this important legislation and in support of the Canadian Association of Chiefs of Police.

There are a number of aspects to Bill C-13 that are supported by the police community, of which the OPP has had an opportunity to provide input since the introduction of the bill last fall. The OPP had representation in and contributed to the cybercrime working group, which is part of the criminal justice coordinating committee of senior officials which advised Public Safety Canada prior to the introduction of the legislation. Detective Staff Sergeant Frank Goldschmidt of the child sexual exploitation section of the OPP was the representative on that group.

We also supported statements made in January 2014 by Chief Constable Jim Chu, the president of the Canadian Association of Chiefs of Police. Now-retired OPP Commissioner Chris Lewis was also a staunch supporter of a previous iteration of this important legislation. We have also tried to do our part to reduce crime and victimization through various public education and awareness initiatives.

The OPP is continually educating front-line officers about issues such as self/peer exploitation so that we can better assist educators, parents, and teens themselves when we are asked for support. The OPP has been developing Internet committees within high schools to educate teens about the serious consequences of self/peer exploitation.

Our people talk about the devastating effects and potential criminal risks associated with this activity. We are also providing information and links to resources, such as www.youthconnected.ca, which has been developed and populated by and for teenagers and, of course, www.NeedHelpNow.ca.

As police, our biggest concern is that teens are unintentionally victimizing themselves by sending inappropriate images of themselves to others. They seem unaware of the consequences when the images often go viral across the Internet or other social media sites. Police are seeing that many teens cannot cope with the shame and embarrassment of what they have done. Many become depressed, anxious, and sometimes suicidal.

The OPP child sexual exploitation unit, on average, receives three to four sexting complaints each week, making it the highest reactive investigative occurrence fielded by this unit. Depending on the individual circumstance of each incident, an offence under the Criminal Code of Canada may or may not have occurred. Offences include possession and distribution of child pornography, extortion, and threatening.

Similar complaints are received regularly by OPP school resource officers and members of the OPP crime prevention section youth issues unit for investigation. The OPP has been a proud supporter and partner of the Canadian Centre for Child Protection and the initiative supported by Public Safety Canada called NeedHelpNow. NeedHelpNow is a web-based resource designed to help Canadian youth, especially in the age 13 to 17 demographic, manage the negative consequences that can occur when sexual images are created and distributed online and to reduce further harm.

NeedHelpNow.ca provides teens with practical steps to regain control over the situation, helpful information about how they can seek support from a safe and trusted adult, and strategies to manage harassment that may occur both online and offline, such as bullying.

The OPP has also been supporting ongoing efforts to call for improved and updated legislative tools to help our police get access to the information we need to investigate child sexual abuse via the Internet, cyberbullying, and other criminal activities using the latest technologies and platforms.

Some of the laws regarding police accessing and using electronic information haven't been updated in more than 40 years. Investigations involving the most vulnerable people in our society, our future leaders, our children, and crimes like online luring, cyberbullying, and self/peer exploitation, or sexting, are time consuming and cumbersome, and in effect, they actually protect the identities of child predators and the materials that they produce.

● (1115)

Thanks to recent legislation, Internet service providers, ISPs—whose own national association, we want to say, view us as their partners—have a legislated duty to report when their services are being used for purposes related to child abuse.

We are still seeking a means to reduce the complexity and the inherent cost of these investigations. Current processes include serving ISPs with a search warrant, a production order, or a law enforcement request for subscriber information relating to a particular Internet protocol address.

Many have raised concerns regarding their personal use of the Internet and privacy of their information. What we want I can liken to using a licence plate number called in as a tip to the police about a dangerous or impaired driver. It's the same thing here. The OPP and its police and community partners believe the Government of Canada's legislation strengthens our ability to obtain vital information quickly, which can then be brought to bear on Internet predators, regardless of their location.

As has been demonstrated by police across North America and around the world, we are making progress in combating Internet child luring, sexual exploitation and abuse, through great police work and information sharing, greater public awareness through

partnerships with third-party agencies, such as the Canadian Centre for Child Protection, in the cybertips program, and by being equipped with ever-improving and legislative tools that need to be modernized to help us keep up with an online society.

Bill C-13, as proposed, will enhance our ability to investigate hate crimes as well.

While the Internet and new communications technologies have true, positive value for us as a society, they also have a downside. These new communication technologies are allowing old crimes to be committed in new ways, and they are fostering the development of new crimes. There is no question, some of the legislation involving technology and communications in Canada is out of date.

I can speak to a couple of important differences at a high level, and perhaps Staff Sergeant Matthews can speak to these on a more specific level during questions. Under the current legislation, police can only access the very basics of subscriber information—name and address, maybe a phone number—on a totally ad hoc basis from Internet service providers. This means there is an inconsistent response which impedes investigations and many times prolongs victimization.

Under the proposed legislation, ISPs will be compelled to provide this information in a timely fashion and on a consistent basis. Access to this information will be strictly controlled and limited to law enforcement officials who would be fully trained in these procedures and subject to auditing and/or reporting processes. The outcome will be that the police can quickly and consistently gain access to information that makes a difference to our effectiveness in investigating and preventing criminal activity and victimization.

We see very few negatives with this bill and the various proposed amendments. Should the legislation pass and be brought into force, the OPP recognizes that we will face an increase in calls for service and case workloads related to the investigation of intimate image offences. The OPP will also face resource pressures from investigating complaints related to these new offences.

Of course, the role of the police isn't to create legislation. That's the job of our elected officials. But, in the interest of public safety, we do sometimes need to enter into careful discussion in a public forum that will help inform and shape these matters. Our role as law enforcement is to respond effectively to criminal activities that have found a particular home on the Internet or have been enabled through new communication technologies. The OPP takes its public safety mandate very seriously.

Members of our Provincial Operations Intelligence Bureau, as well as the OPP Organized Crime Enforcement Bureau and the child sexual exploitation unit, take an intelligence-led, coordinated approach to share and leverage information on criminal activities. It takes this intelligence-led, integrated approach with our partners in policing and continued advocacy for the legislative tools needed to meet the law enforcement challenges of today.

We have not been shy about underlining the need for updated legislation that will give us effective tools allowing us to prevent and investigate criminal activity. We do appreciate the federal government's support to enhance what we do to prevent vulnerable persons from being exploited and victimized and to keep our communities safe.

Thank you.

● (1120)

The Chair: Thank you, Mr. Pardy, for that.

Our next presenter is from the Royal Canadian Mounted Police, Commissioner Oliver.

A/Commr Joe Oliver (Assistant Commissioner, Technical Operations, Royal Canadian Mounted Police): Mr. Chair, and hon. members of the committee, thank you for the opportunity to provide an overview of the work being done by the RCMP to combat cybercrime, including cyberbullying.

[Translation]

I am Assistant Commissioner Joe Oliver and I am responsible for overseeing the RCMP's Technical Operations Directorate. Technical operations provides direct specialized investigative and operational services to front-line police officers, including the national coordination of investigations involving the online sexual exploitation of children and the provision of specialized investigative tools to address criminal conduct on the Internet.

● (1125)

[English]

Joining me today is Inspector Mercer Armstrong. Inspector Armstrong works in the policy and compliance unit of the RCMP's contract and aboriginal policing directorate. This directorate is responsible for investigative policy, including that governing enforcement of the Criminal Code. That includes incidents such as cyberbullying in RCMP contract jurisdictions across Canada. Contract and aboriginal policing also monitors RCMP educational and outreach initiatives with respect to the prevention of cyberbullying and other crimes.

I would like to start by discussing cybercrime more broadly. Following this, I will touch on some of the investigative challenges that police face in the digital era: challenges that relate to the anonymous, hard-to-detect, and often cross-border nature of cybercrimes. I will then address specific forms of cybercrime that have a devastating impact on youth, namely cyberbullying and the non-consensual distribution of intimate images.

When it comes to cybercrime, it is important to note that cybercrime is, in many cases, a modern means to commit familiar crimes. For example, criminals create and deploy malicious software programs to steal passwords or to obtain personal and financial

credentials. This information then allows them to commit a number of offences, such as fraud, identity theft, and other financially motivated crimes. Recently, the RCMP worked with its international partners to investigate the deployment of malware that infected thousands and potentially millions of computers for such criminal purposes. As part of Operation Clean Slate, the RCMP investigated offences involving the unauthorized use of computers and mischief in relation to data, sections 342.1 and 430 of the Criminal Code, respectively.

These provisions, however, do not fully address key elements of cybercrime, including the possession of a computer virus for the purposes of committing mischief, or importing or otherwise making computer viruses available. These criminal threats come from within Canada and abroad, are carried over Canadian telecommunications networks and, in many cases, are both a threat to Canadians and to our allies. As it stands, the Criminal Code's coverage of unauthorized computer use and data mischief does not fully reflect the magnitude of today's cybercrime environment and the potential scope of related police investigations.

In the fight against cybercrime, timely securing digital evidence in a virtual world is critical. As we all know too well, computer data can be easily altered or deleted, whether inadvertently or intentionally. During the course of a cybercrime investigation, Internet service providers may delete computer data, and therefore potential evidence, as part of routine operations. Law enforcement, as part of common law policing duties, may request service providers to voluntarily preserve data. Notwithstanding this measure, police forces currently have no means of ensuring that service providers do not delete when there is a reason to suspect criminal activity, whether through short-term demands by a police officer, or longer-term orders by judicial authorization. The absence of such investigative tools puts potential evidence at risk as investigators develop their case in support of meeting judicial thresholds for data access.

[Translation]

Another digital evidence challenge relates to the issue of attribution. In other words, how do we start to identify a potential suspect in an online context, particularly when a suspect may have taken sophisticated steps to disguise his or her digital tracks through anonymous online networks, encryption technologies or other cyber-related measures, such as a botnet?

[English]

In that context, specific components of digital evidence, such as transmission data or tracking data are particularly important at the start of a police investigation into online criminal activity. These very precise types of digital evidence allow police to potentially attribute online criminal activity to a source and further investigative leads. Currently specific types of data such as transmission or tracking data may be obtained through voluntary disclosure by a third party or through judicially authorized general production orders or search warrants.

In the case of general production orders or search warrants, police must meet the standard of reasonable grounds to believe that a crime has been committed. This standard can be challenging to meet in the early stages of an investigation where an officer may have reasonable grounds to suspect online criminal activity, but nothing else. In such cases specific forms of data, such as the ones I've mentioned, may contain critical early indications of criminal activity, indicators that are often necessary to commence effective police work in the cyber realm.

These investigative challenges are by no means limited to financially motivated crimes. They extend equally to other devastating online crimes that target our youth such as online child exploitation and cyberbullying. Youth are one of the RCMP's strategic priorities, and comprehensive strategies including education, awareness, and enforcement initiatives are employed to prevent youth victimization and to respond to the participation of youth in criminal activity.

For example, the RCMP's National Child Exploitation Coordination Centre, one of the areas within my portfolio, works with law enforcement partners across Canada and internationally to combat the online sexual exploitation of children. The centre also works closely with the Canadian Centre for Child Protection, a charitable organization that operates Canada's national tip line, cybertip.ca, for reporting online child abuse and sexual exploitation incidents.

To address cyberbullying the RCMP's Youth Resource Centre provides officers working in over 5,000 schools across Canada with lesson plans and related educational tools to help youth recognize, respond to, and prevent both traditional bullying and cyberbullying behaviour. In addition the RCMP's National Crime Prevention Services has also partnered with PREVNet, a national network of researchers and organizations working to stop bullying and cyberbullying, and the University of Victoria to pilot WITS, an acronym for walk away, ignore it, talk it out, and seek help. The WITS program aims to prevent peer victimization and bullying, including cyberbullying, through youth engagement. The pilot is currently supported in 50 schools and has engaged over 8,800 students. These activities are fundamental preventive measures to address cyberbullying.

Unfortunately, cyberbullying cannot always be addressed through prevention. As identified by the cybercrime working group of the coordinating committee of senior officials, bullying and cyberbullying may be manifested in a range of criminal offences, such as criminal harassment, uttering threats, or intimidation. High-profile cyberbullying incidents have taught us that bullying may be facilitated and amplified by telecommunication. As it stands, the existing provisions in the Criminal Code regarding offences of false, indecent, or harassing communications do not currently reflect the increasingly ubiquitous role of telecommunication as a possible medium to bully individuals in a criminal capacity.

Recent incidents of cyberbullying, specifically those involving the non-consensual distribution of intimate images, come with other investigative challenges too. For example, for victims under the age of 18, the use of child pornography provisions to charge individuals may be challenging to align with the intent of these offences. As the previously mentioned cybercrime working group identified, it may be viewed as too blunt an instrument to address the non-consensual distribution of intimate images, especially in situations where the offender is also under the age of 18. These current parameters may have a limiting effect on the investigator's discretion and options in proceeding with appropriate criminal charges.

(1130)

[Translation]

In closing, many cyber-crimes are essentially very sophisticated ways of committing recognizable offences: theft, fraud, bullying, extortion or child exploitation to name a few. But the criminal use of information technologies, however, creates significant challenges for police investigations.

These challenges include the preservation of evidence, the difficulty in identifying and attributing criminals online, or standards of proof more fitting to "real world" investigations in physical, "noncyber" domains.

[English]

Steps to modernizing offences and investigative tools in the Criminal Code would permit Canadian law enforcement to better address criminal forms of bullying and other crimes in the digital age. I would also emphasize that steps to harmonize Canada's criminal laws and investigative tools with those of its allies would enable the RCMP to more effectively work with international law enforcement partners in addressing the many online crimes that are transnational in character. Bill C-13 would help to address investigative challenges that I've mentioned.

Inspector Armstrong and I look forward to answering your questions.

The Chair: Thank you very much for that presentation.

Our next presenter is from the Halifax Regional Police, Chief of Police

Chief Blais, the floor is yours for ten minutes.

Chief Jean-Michel Blais (Chief of Police, Halifax Regional Police): Thank you very much.

[Translation]

Good morning, Mr. Chair, and ladies and gentlemen of the committee.

My name is Jean-Michel Blais and I am the Chief of Police, Halifax Regional Police Service. Unfortunately, I was not able to join you today in Ottawa, because my schedule is quite full and I have other commitments. However, given the subject you are studying, I am going to testify by videoconference.

• (1135)

[English]

As the Chief of Halifax Regional Police, I am honoured that the committee is giving police and my service an opportunity to lend our voices to this important issue. I would also like to thank Chief Chu for extending an invitation to me to participate in this discussion.

As a member of the Canadian Association of Chiefs of Police and as a chief of police whose community has seen first-hand the devastating consequences of exploitative online behaviour, I fully support the introduction of Bill C-13. It will serve to improve online safety, allow for the effective investigation of Internet and technologically-based crimes, and provide consequences for cyberbullying and the non-consensual distribution of intimate images. With the advent of the Internet, no one could have anticipated the pace of technological advancements or the implications they would have on our society, particularly our youth, who are digital natives as opposed to us, a bit older, who are really digital immigrants.

In this technologically evolving landscape, we in policing are currently faced with some laws that were adopted in the rotary telephone era. We require modernized laws, as proposed in Bill C-13, which reflect the Internet era so that we can more effectively investigate and prosecute those using the Internet and other related technological platforms for a criminal purpose. In short, we need laws that recognize more modern forms of technology that did not exist when certain dispositions of the Criminal Code were first created. Furthermore, we require laws that modernize the investigative tools police can use to detect and combat crime while maintaining citizens' right to privacy. Bill C-13 will do that by providing a set of tools that will allow us to be effective and efficient in conducting investigations in today's high-tech environment while at the same time maintaining the judicial checks and balances needed to protect Canadians' privacy.

I want to share with you some examples from my investigators as to how Bill C-13 will strengthen police investigations and better serve our citizens and our communities. Today, as you know, there is no provision in the Criminal Code to address a person sending or posting intimate images of a person without that person's consent. This has become an increasing problem in society where, given the proliferation of social media, adults and children have becomes victims of cyberbullying and harassment through the non-consensual distribution of their intimate images. The proposed amendments would change that, better protecting all citizens from such acts.

The provisions of Bill C-13 will also provide investigators with the option of charging offenders with the non-consensual distribution of intimate images rather than child pornography offences in circumstances where the image is of a person under the age of 18. We view this of high utility in cases where the offender may also be a youth who, given their age and maturation, may not fully realize the devastating consequences of their actions, yet could currently face a criminal record for child pornography offences. Today's laws

were not crafted with that intent in mind, and police believe that the provisions in the proposed amendments provide a more measured and appropriate approach and response in such instances.

On a personal level, I remember in 2003 when I was in charge of Manitoba's integrated child exploitation unit, all of our suspects were males in their 20s and 30s from various backgrounds. Some lived in their parent's basements while others were successful investment dealers and professionals of all stripes. If we had been asked then what the future would reserve for us, we would never have thought that in ten short years, people, including children, would be able to transmit graphic images that would constitute child pornography or result in some form of harassment simply through the use of a hand held cell phone.

This leads me to ponder, as both a police executive and a father of three children, as to what technologies have yet to be created that could result in further exploitation of children and adults. With C-13, it is proposed that offences involving harassing and indecent phone calls be changed to reflect modern means of communication to include harassing and indecent communication, broadening the scope of the offence to reflect today's technologically advanced milieu.

Police will be able to make traditionally sanctioned preservation demands and obtain preservation orders to secure data by telecommunication service providers or social networking sites until such time that investigators are able to obtain a production order or a search warrant to legally obtain the evidence. Currently, information can either be deleted or unpreserved by these entities as there is no legal obligation for them to do so. This is compounded by increasingly shortened data retention periods due to the inconceivable amount of data generated on today's technological platforms.

As I mentioned earlier, online exploitation has had devastating consequences here in Halifax, the effects of which reverberated around the world. To echo Chief Chu, we recognize that changing the law is only one part of the equation. But this bill, when it is coupled with education, awareness, and integrated community services, is a significant step forward in helping police and the community at large to effectively and efficiently deal with cyberbullying and the non-consensual distribution of intimate images, acts that perpetually revictimize the victims.

Ideally, when education and awareness approaches ultimately fail, the justice system must be properly equipped to respond. Nova Scotia has been at the fore of this issue, with introduction of the Cyber-safety Act just over a year ago. This, coupled with the law amendments of Bill C-13, will provide a powerful combination in addressing criminals who exploit or harass the vulnerable online.

As police agencies deal with cyberbullying and the perpetually expansive use of the Internet to commit other cybercrimes, we owe it to all such victims to be able to adequately investigate these files. We must fulfill an advocacy role for all Canadians and send the message that we will no longer tolerate the online victimization of our citizens.

It goes without saying that, as men and women respectful and ever-mindful of their imperious obligation to the rule of law, this must be done in such a way so as to respect the privacy rights of all Canadians. It is for that reason that we at Halifax Regional Police lend our support to this important and required legislation.

Thank you again for this opportunity.

(1140)

The Chair: Thank you, Chief.

Now we will go to our rounds of questions.

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

[Translation]

Ms. Ève Péclet (La Pointe-de-l'Île, NDP): Good morning, ladies and gentlemen. Thank you very much for being here today. Your presentations were all very interesting. I am very pleased that each one of you mentioned the need not only to act following an offence, but also to try to prevent that offence through education and awareness. I congratulate you for the programs you have mentioned and I thank you for your work.

If any of you want to say something or to complete the reply of one of your colleagues, please feel free to do so.

My first question goes to Mr. Oliver. In your presentation, you talked about cyber crime in general. We know that Bill C-13—[*English*]

targets just the particular infraction in the non-consenting distribution of personal images. How would you proceed with a different kind of cyberbullying? This is just a particular infraction that we're targeting right now. It's only the distribution of personal images without consent. But how would you proceed with a different case of cyberbullying? Do you have the tools to proceed, for example regarding an individual who would bully someone by text messages or Facebook messages. How would you proceed?

[Translation]

A/Commr Joe Oliver: Please allow me to answer in English.

[English]

For cyberbullying, a number of existing Criminal Code offences potentially apply, including criminal harassment, uttering threats, mischief in relation to data. In addition to a new offence of publication of intimate images without consent, Bill C-13 also amends other provisions to modernize them, provisions, such as section 342.1, when it talks about "imports, obtains for use, distributes, or makes" available—for instance, the unauthorized use of a computer.

Some forms of harassment or revenge include taking over someone's computer, posting images that appear to be coming from them, and those types of things. In those cases, you're involved in more sophisticated investigations that would have to prove the origin of the virus or the defacing of somebody's website. Now in order to do that, in modern day communications, some communication would travel through multiple networks and through multiple service providers.

As for tools that are offered in Bill C-13, I just want to clarify that there are no provisions in here to give warrantless access to information to the police; all of the proposed investigative measures require prior judicial authorization. So in the case of trying to identify where an attack originated from, there is the communications trace production order that would allow us to identify, by hopping through the network, the service provider that actually may possess content. Then we may obtain a production order to actually find the content and details of the offender. So there are a number of means within this investigative toolkit that is being proposed in Bill C-13 that would assist in other forms of bullying. But I must also emphasize it would also assist in other forms of cybercrime.

• (1145)

[Translation]

Ms. Ève Péclet: Mr. Chu, if I may, you mentioned the difficulty of conducting investigations because the Internet knows no borders. It is not actually like an offence committed in the street. You mentioned websites that are about "revenge porn" and things like that. But clause 5 of the bill provides for a procedure to order the closure of that kind of website containing intimate images. But the server where the images are stored has to be on territory that is under the jurisdiction of the court issuing the order.

Would it be possible to order those kinds of sites to be shut down? What would be the proper procedure? Are you sure that this bill gives you the tools you need to conduct investigations of that kind?

[English]

Chief Jim Chu: Yes, some of these websites that I mentioned actually have a legitimate purpose for a legal exchange of information or communication. However, when someone decides to engage in criminal behaviour using that website as a legal channel of communication, that's where the problem resides. So if we asked a website such as ask.fm, for example, based in Latvia, who posted something or was the user or account holder, they would not cooperate with Canadian law enforcement. They wouldn't even answer our e-mail.

That's where we get back to what my colleague, Assistant Commissioner Oliver, mentioned. Then we would look at by what routing the IP address arrived at, which may identify the fact that the person who originated the e-mail or posting resides in the same city as the victim. Then we can proceed further and get those production orders to find out who owns that account.

So the crime begins with the person. They may use something overseas, but these tools help us to trace it back to the person who did the crime.

The Chair: Thank you very much.

Thank you for those questions and answers.

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

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

And thank you, gentlemen, for being here.

My first question is for the chief of the Halifax police. Unfortunately, we've heard from victims that in the early stages of incidents of cyberbullying, there is no recourse for the police in some cases. In other words, without Bill C-13 the police are relatively limited when it comes to the widespread non-consensual circulation of intimate images.

Do you believe that the police require additional tools to do their job in order to protect people from the widespread non-consensual distribution of intimate images? Furthermore, from the position of front-line police officers, can you speak about your experience with cyberbullying cases or specific cases that deal with the distribution of non-consensual intimate images at the early stages?

Chief Jean-Michel Blais: Yes, thank you very much, Mr. Wilks, through the chair.

The question for us here is one of time. It's about being able to ensure that, once we have identified where or what that information is, we can be able to properly obtain that information before it gets deleted, first, and before it gets lost, second. You can well appreciate now with the amount of data that is being developed by various sites and within the Internet as a whole, that we're talking about a massive amount. To be able to go back four, five, or six months after the fact, is very challenging. Of course, that being said, the key is to be able to get that information and to get it in such a way that we can bring it towards a proper judicial conclusion in the courts.

With regards to additional tools, what we've experienced on several occasions is individuals who have come to us saying that a photo of their daughter or themself is now on the Internet. Very often, what they're looking for is that the image be taken down. We do not have the tools right now. To be honest with you, I don't even know if those tools can really exist.

From my experience in having worked in child exploitation in the past, the biggest challenge we have is the perpetual revictimization of victims on there. So to answer directly with regards to being able to take them down, it's very difficult. Yes, we can identify certain individuals who may have that image, but as you can well appreciate, and I'm sure many of you follow Twitter, once you tweet a message, it can go all around the world in a matter of moments.

● (1150)

Mr. David Wilks: Thank you very much for that, Chief Chu, and Assistant Commissioner Oliver.

As we're all aware, evolving computer and communications technologies have made some crimes easier to commit and harder to investigate. In Canada, crime is currently being investigated using practices that do not always reflect the emergence of these new technologies. You alluded to part VI. Being the author of an affidavit back in the day, I can attest that it took 732 pages and a year and a half to get there. In this day and age we need to move more quickly. It is our government's position that our laws need to be modernized to allow for more effective and efficient responses to crime.

Can you comment on the need to update the Criminal Code, and how does an outdated Criminal Code affect the day-to-day work of police officers?

Chief Chu, you first please, and then Assistant Commissioner Oliver.

Chief Jim Chu: Well I understand that the economics of policing is a major focus for the federal committees and government to study. Policing is expensive, and we only have so many police officers. If they're forced to engage in cumbersome processes that take extensive amounts of time to get information that turns into a dead end, then those are situations where those investigators can't work on other cases.

Quite frankly, there are certain types of investigations when we look at the probability of a solution and we don't follow up on them, especially if they involve an international element. However, there are also local cases that I think we can be more nimble with and investigate them more quickly, helping to prevent more victims from being harmed, if we're able to react quickly more quickly.

A/Commr Joe Oliver: Thank you for the opportunity.

Well, I could touch on a couple of components that will talk about what Bill C-13 will do in modernizing investigative tools.

First of all, in my opening remarks I spoke about preservation. Today we are completely reliant upon the voluntary cooperation of entities when it comes to the preservation of data. To allow time for the police to actually develop the production order or a tracking order of some sort to acquire evidence and pursue an investigation further, as proposed in BillC-13, the police would be able to make a preservation demand of service providers, which would allow us time then to pursue an investigation. And particularly when one speaks of international partners as well.... If it's a domestic investigation, we would have 21 days to prepare a production order. Often we are cooperating in this borderless world of the Internet. It allows 90 days for us and the Department of Justice to work with the International Assistance Group and their international partners to obtain a production order in that process.

The preservation order is another tool that can be used to to preserve the data so that we could then turn to the other means that are available in this bill and in the Criminal Code to obtain more evidence.

With respect to some of the other provisions, they modernize the investigative tools available, and in certain cases they recognize the importance of privacy. Take, for instance, a tracking device. Today, police, under section 492.1, can secure a tracking device in order to monitor location and movements of a thing, which would assist in real-time surveillance, and corroborate other information that we may have during an investigation. It's recognizing the importance of privacy. In the current regime that would include installation of some sort of tool on a mobile device to track an individual, and the threshold there is "reasonable grounds to suspect". Under the modernized bill that actually increases the threshold for police to "reasonable grounds to believe". So when it comes to a device that is normally carried or worn by an individual, let's say a cellphone, the threshold for tracking under Bill C-13 has actually increased the threshold.

• (1155)

The Chair: Thank you, Assistant Commissioner. It's time.

Thank you for those questions and answers.

Our next questioner from the Liberal Party is Mr. McKay.

Hon. John McKay (Scarborough—Guildwood, Lib.): Thank you, Mr. Chair.

I'm going to operate at a bit of a disadvantage since I'm not a regular member of this, Chair.

I was interested in your comments, Commissioner Oliver, about tracing it back to the originator of an image, which seems to me to be the core of the issue. What's not clear to me is how you trace it back. Do you have to go through his computer and his computer and her computer and my computer to get back to wherever the computer is that started this chain? If you are doing that, are you doing it with a warrant, or without?

A/Commr Joe Oliver: The new provisions would allow for new tools that would allow the production of communications trace.

Hon. John McKay: So this is proposed section 164.1?

A/Commr Joe Oliver: No, it would be proposed section 487.015, that is, the communication trace production order.

A communication trace production order implicates historical information in a situation where the originating service provider may not be known. So in some recent investigations when there's been an exfiltration of data—let's say someone stealing credentials—we're able to identify where that came from. But then we go to that service provider, and they say it actually originated somewhere else. So then we keep going to the service providers, hopping to the point that we actually identify the original—

Hon. John McKay: So you're hopping from service provider to service provider, and not necessarily from computer to computer.

A/Commr Joe Oliver: Precisely.

That is one tool now being offered under this new legislation. The other is production of transmission data, which is proposed section 487.016—again, historical. In this case the service provider is known. We can go back to a computer. Let's say there was an attack and we know the service provider. It was Rogers. We can obtain a production order in this case. Now, what we're saying is, "We believe one of your accounts here was involved in an attack." And what we want to see is their historical data, to actually capture the evidence of....

Hon. John McKay: What is Rogers' obligation at that point to tell you that the originator is X or Y?

A/Commr Joe Oliver: The transmission data is very precise. It contains no content on transmissions. It does not reveal substance, the meaning, or the purpose of the communication. It more or less identifies a type direction data—the date, duration, and so forth. So it's actually similar to phone call data today. If I were to make a phone call I know that this number called that number. So it' the same thing with this computer calling that computer. So we're establishing the link.

Hon. John McKay: Is there any involvement of a judge at that point?

A/Commr Joe Oliver: All of these provisions in Bill C-13 require prior judicial authorization. There are no warrantless access provisions in this bill.

• (1200)

Hon. John McKay: Chief Chu talked about section VI, and unlike Mr. Wilks, I've never prepared a 700-page document. What's involved in preparing that kind of material for a judge to warrant the police to go from server to server?

A/Commr Joe Oliver: The threshold, as proposed in the legislation here, is reasonable grounds to suspect.

Hon. John McKay: I assume the threshold to anything else, really....

A/Commr Joe Oliver: The police would have to identify the leads on the investigation. We actually have to set out what we know about the complaint, about the potential criminal violation, as well as any information we have that convinces a judge that we have reason to suspect that this telecommunication service provider may have hosted a transmission that was involved in a criminal activity.

Hon. John McKay: Let me just turn to Chief Blais for a second. I'm working on the assumption that because you're from Halifax that you were eminently involved in the Rehtaeh Parsons case. Where was the big gap in police authorities, criminal authorities in order to conduct an appropriate investigation in that file?

Chief Jean-Michel Blais: Well, you can well appreciate that presently the file is before the courts, number one, and number two that there will be a review that has been mandated by the province. I can't talk in specific terms with regards to that file, but I will try to answer your question by mentioning some of the problems that we have in general.

It's a question of getting the information in a timely matter. We've had several other cases whereby we've made requests to IP providers out of the states. Facebook, for example, we have to go through an MLAT process and that could take upwards of several months. That's one of the big challenges that we've had as well.

Hon. John McKay: Will this bill actually address that?

Chief Jean-Michel Blais: It would to a certain measure, but I think what it would allow us to do is that once we identified specific information and were able to determine where that information was housed, for example, as indicated before, we'd have that 21-day period if it's a local provider to be able to get that information now. If at the end of that 21-day period we weren't able to get the necessary judicial authorization in place, then it would fall and we wouldn't be able to obtain that information. It would help us. I don't think it would go as far as we'd like it to in order to get that timely information, and timely, ideally, would be within the days that would follow. But as indicated before, we also realized that when we are doing these documents, something as simple as a search warrant is no longer simple today.

The last search warrant I wrote was back in 2002 and it was a 15-page document. It took me about three days to prepare and that was simply for a public mischief charge.

Hon. John McKay: Is the 21 days an impediment that could be addressed at this stage?

Chief Jean-Michel Blais: It could be, but once again, if we don't have that information, especially with the thresholds being reasonable grounds to suspect, then we may never have that information. I think as legislators you have to make that decision as to what is the best threshold and timing in there. We have to be fair to the Canadian public that we must be able to have all of the information that is there. As Chief Chu alluded to regarding the economics of policing or public safety, we have to be able to [Inaudible—Editor] the necessary resources to get the work done.

The Chair: Thank you.

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

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

Ladies and gentlemen, I really appreciate your being here today and taking us through some of the very technical parts of this bill relating to the tools that the police need to investigate these crimes, which I think everyone agrees are serious and have, as one of you said, a devastating impact on people.

Chief Chu, I'd like to ask you a question regarding the current policing process for these types of offences and how you would see things change if this bill passes. If I could just give you a hypothetical case, a young person has a conversation over the Internet with another person but doesn't have any way of verifying the identity of that person, and in relation to that discussion over a period of time, the young person sends an image of themselves to that person and subsequently that person threatens to do something with it. The young person then realizes that person is not a friend and is worried. If they come forward to their parents or a teacher and either the victim or one of those other people contacts the police today, what do you do? What can you do to find the identity of the person who has the image and is threatening to do something with it?

● (1205)

Chief Jim Chu: The question you ask is a common scenario. Our school liaison officers dread Monday morning when the kids march into their offices and talk about what happened over the weekend.

In the example you provide of text messages and threats conveyed that way, sometimes we don't have a name. The person is anonymous, but we may have that IP address, which as mentioned earlier, may come from one provider. Then we can use the provisions under the new Bill C-13 to quickly and nimbly get a production order for tracking where that originated and eventually we come back to a suspect. Once we have that suspect—it could be a predator based in California—we would then engage in an international investigation using multilateral assistance.

However, It may be just a classmate, and the victim had no idea who it was. For us to quickly identify that person allows us to intervene to stop it from happening. Quite often a warning is sufficient. If it is more serious and involves intimate images, again, we now have the ability to lay not as serious a charge as child pornography distribution, but the new provisions in Bill C-13.

Mr. Bob Dechert: Okay, today do you contact telecommunications service providers when conducting that kind of an investigation?

Chief Jim Chu: Yes, our organization has one central point of contact. Every investigation in the front lines goes through one coordinator, and she talks to the telcos.

Mr. Bob Dechert: Do you have the right to compel that ISP to give you that information today?

Chief Jim Chu: The only way we can compel them is to appear before a judge and obtain a production order.

Mr. Bob Dechert: Will that change under the new legislation?

Chief Jim Chu: Often when we just want the tracking information, it's easier for us to write a production order when we only have to articulate grounds to suspect, and quite often that's going to be a dead end. If it's a Wi-Fi café, that's good, because we don't then waste three days writing the full production order when we didn't even need the other data.

Then we also have the ability to tell the telecom companeyt that we want them to preserve that evidence. That's a very powerful tool now. Then if we are required to go back with a full production order, the evidence is still there; it hasn't disappeared. These warrants take several days now. That's one of the concerns we have with a general production order, but that's the way it is.

Mr. Bob Dechert: You mentioned that things can move very quickly over the Internet. Do you believe—and I'll ask this of any other officer who wants to respond—that people have a right to be anonymous on the Internet if they're sending messages to other people?

Chief Jim Chu: I don't believe people have the right to be criminals on the Internet, and if they engage in crime, then we need the means to identify them and stop them, arrest them.

Mr. Bob Dechert: Okay, if the young person who is the victim in the scenario I proposed comes to you and says they're worried that this other person whom they don't know might do something with that image and cause great damage to their reputation, do you feel that person at that point has a right to maintain his anonymity—not the victim, the other person?

Chief Jim Chu: No, not at all, because once somebody crosses the line from collegial banter back and forth to they've broken a law by trying to extort or defraud, we need to identify that suspect.

Mr. Bob Dechert: So if you ask an ISP provider for that information today, and they give that information to you, and then you contact that person and say, "Stop using that image; don't do anything criminal with that image," should that ISP provider bear any liability if it turns out that the victim was wrong about the criminal intention of the other person?

● (1210)

Chief Jim Chu: When we go to an ISP provider, we outline why we're asking for the information. There's a form we fill out, it's a legitimate law-enforcement purpose. Many Canadians want to help the police; there are many situations where citizens will tell us who rented the apartment last week, or who rented that car yesterday, and some of these telecommunication providers will help us, because they don't want their networks to be used for crime.

Mr. Bob Dechert: Sure, it's kind of like, as I think Officer Pardy said, if you see a car driving down the street and you suspect that the driver is impaired, you can copy down the licence number and provide that to police. I assume the police can also ask you for it. If I see, today, somebody harassing one of my neighbours on their front porch, and there's a car in the driveway, I assume I can note down that licence number and provide it to police, and by the same token

the police can come to my door and say, "Did you see somebody harassing your neighbour; do you have any information that would lead us to that person's identity?" That's true? Okay.

Chief Jim Chu: A better example is, you have a basement suite, and we come to you and say, "This person committed a crime last month; what's the name of the person who rented your basement suite?" If you said, "I need a production order," that would take a lot of police time over the years.

Mr. Bob Dechert: Should it be any different with respect to information sent over the Internet?

Chief Jim Chu: The telcos do tell their customers when you sign up for the service not to use their communication channels for crime."

The Chair: Thank you.

Great questions, good answers....

Thank you very much.

Next from the New Democratic Party, Mr. Garrison is here with us today.

Mr. Randall Garrison (Esquimalt—Juan de Fuca, NDP): Thank you very much.

Thanks to the witnesses for being here today. I know many of you from the public safety committee, where we're used to seeing men and women in uniform.

I know we have broad consensus in Parliament that there's a necessity to act against the non-consensual distribution of images, but there's a lot more in Bill C-13than just that, so I'm going to focus on some other aspects in my questions.

We certainly heard from the witnesses today your case for updating the Criminal Code and having new tools to respond so you can get timely access to information for investigations of cybercrime. But we've also heard concerns from other witnesses and other members of the public that in providing those tools, Bill C-13 is sometimes overly broad. So I want to focus on the question of lawful access.

Bill C-13 creates the new tool of a preservation demand or a preservation order for data, and I'm probably prepared to concede that may be something that you need to have, but why does the standard of proof change? Why shift from reason to believe to the lesser standard of reason to suspect? Wouldn't this tool still operate at the higher level? Wouldn't it still be a good tool if it was reason to believe?

I guess I'll ask Mr. Chu, as the president of the Canadian chiefs association.

Chief Jim Chu: A warrant or production order that has to satisfy reasonable grounds to believe is a very onerous standard to meet, and rightly so. That's a level of an order that we would need to see the private information. If we simply say, "Look, please hold it and let us go away and do some work," we may find out that we don't need to come back and access all of that information. That actually then helps us move forward with our investigation quicker.

Mr. Randall Garrison: If you can't meet that higher standard wouldn't that, I guess, do the same thing? In other words, you may be pursuing a case that won't have any future if it can't meet that higher standard.

Chief Jim Chu: Once we preserve the data, then we're doing more investigation. We're talking to more witnesses. We're examining other aspects of the case, and if we find that we don't have enough information to go get the full production order, then that data is deleted and there's no intrusion into that person's private data. But if we do fortunately come up with the necessary evidence to satisfy the judge, then the evidence hasn't disappeared, which is our concern

Mr. Randall Garrison: But doesn't the same thing happen in all kinds of other police investigations, I mean you have that higher burden of proof before you can do things everywhere else? Isn't that a common problem, or is this something you would say is specific to cybercrime?

I don't know if Commissioner Oliver wants to jump in on that.

A/Commr Joe Oliver: I would just add that the threshold of reasonable grounds to suspect is not unfamiliar to the Criminal Code. In fact existing provisions in the Criminal Code already have that threshold. But other provisions, because they're more intrusive, have "reasonable grounds to believe" threshold.

I think the important aspects in these cases are when it comes to preservation. We're not acquiring any information at the time. What we're asking is: hold that, we're coming back. We think a crime has been committed, but let us go away and gather more evidence so that we can come back with the proper production order, so that the evidence is preserved and is available for us to see at a future point.

But other provisions, such as going to a financial institution to obtain the name and account information of a person, exist at the "reasonable grounds to suspect" threshold. A tracking device today is at a "reasonable grounds to suspect" threshold, as is dial number recorder, which is consistent with the new tools that are being offered here, with the exception.... Actually, in one provision the threshold is actually increasing when it is a device that I would normally carry on myself. Recognizing that potential intrusiveness of that, I think the drafters increased the level to reasonable grounds to believe.

(1215)

Chief Jim Chu: I have a better analogy for your question.

If we were in a position where we had to search a house and we had to get a search warrant, we could guard the house physically, and then go get the search warrant, and then come back with the warrant and search the house. Cyber-information could disappear.

Mr. Randall Garrison: Okay.

It seems that Bill C-13 expands access to some of these tools beyond peace officers. Chief Chu raised the example of mayors, but there's something actually more specific in the act. In its definition of who might access some these tools, it mentions public officials who administer and enforce any act of Parliament.. It says that in a couple of places. I guess I'm asking you the obvious. You don't really need that, do you? "Peace officers" would cover anybody that you need, so I'm not sure why the bill expands it to any other administrator of a federal act. It wouldn't affect your work. "Peace officers" certainly covers everyone you've got.

Chief Jim Chu: We can only speak for law enforcement here.

Mr. Randall Garrison: Well, I'm asking you a kind of obvious question, that "peace officers" covers—and, in fact, quite broadly—anybody who would be in a position to make use of these powers....

Chief Jim Chu: That would cover CACP members, yes.

Mr. Randall Garrison: Okay.

The last one, and you may give me the same answer, but in this act it appears to expand some of the immunity for service providers for some of their voluntary actions. I have a question about why that happens, and you may not be able to answer this. If the police already get a tool where you can get preservation of data, at request, really, then why is there is a broad immunity to the service providers being provided for voluntarily doing so? You may have needed it before, when you didn't have the power to ask for it, but why now would that immunity be necessary?

Chief Jim Chu: It's our belief those immunity provisions already exist. It's just a housekeeping measure that was thrown in. But under the law and under case law, it already exists.

Mr. Randall Garrison: So you don't believe that this really changes the real situation on the ground, Commissioner Oliver?

A/Commr Joe Oliver: I would just echo the views of Chief Chu that the provision already exists in the Criminal Code.

My only commentary is that, and I'm not speaking specifically to this issue, the Canadian policing model is developed on the notion of the police are the community and the community are the police. The reality is that the police cannot operate in a vacuum, where we compel everything. We have to rely on the cooperation of citizens, witnesses, and third parties all the time in our investigations. There was an example provided earlier about an armed robbery that may have taken place in a shopping mall. We may have witnesses that observed that, if they come to the police and provide information to us, the mall may have video that we go and try to acquire. We're trying all of these things in a timely manner, because if this is particularly a serial robbery team, then we want to get on that team as soon as possible.

If someone is prepared to cooperate, we see that as fundamental to policing in Canada. It's a partnership to community safety.

Mr. Randall Garrison: Thanks very much.

The Chair: Thank you for those questions and answers.

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

Mr. Patrick Brown (Barrie, CPC): I think my colleague, Kyle Seeback, wants 30 seconds.

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

When we're talking about the preservation demand, which is what Mr. Garrison was talking about, and the concern about the lower threshold, which is reasonable grounds to suspect, I think you answered it quite clearly, but I just want to be sure.

The preservation demand just preserves the data for a limited amount of time, and then if the police want to come back and see that data, they have to then get a production order, which is at the higher standard, which is the reasonable grounds to believe, right? It's just to preserve at a lower threshold as part of what may become an investigation. Is that correct?

● (1220)

Chief Jim Chu: That's correct.

A/Commr Joe Oliver: That's correct, depending on the type of information we're seeking.

If it is just looking for the hop between networks—we rely on other new provisions in here—without any personal information, just the communication between different networks, that could be at the "reasonable grounds to suspect" level. However, other provisions would be at the "reasonable grounds to believe" level.

It all depends on the circumstances and the precise.... And that's the clarity of these tools. They're very precise in what they allow us to do. So the definition of "transmission data" and what it includes is very clear.

Mr. Kyle Seeback: That's great, thanks.

Mr. Patrick Brown: Thank you.

I guess one of the challenges is how fast technology evolves. I think, based on what we've heard before this committee, it's fair to say cyberbullying is on the rise, unfortunately. When we think of some of the means whereby things can be communicated really quickly, we're talking about having Facebook and obviously Twitter, but talking to younger cousins or younger friends, one thing I learn is that there is always something new. It's incredible how widely they're used. I just looked up Snapchat, and it said 700 million photos and videos are distributed every day. The target audience is teenagers. Does this bill give you the tools to keep up with technology? Because what we're dealing with today could be just as difficult or even harder a few years from now. We know that app certainly has impressions, when you talk about concerns about the distribution of intimate images, obviously some of those users use tools like that. How do you keep pace with this evolving technology, and is this bill adequate to do that?

Chief Jim Chu: This bill is definitely in the right direction. It modernizes many parts of the Criminal Code that in reality bear the nature of the crime that's committed in an online environment. Five years from now we may have to come back to Parliament and ask for different legislation, but for today it's a great start.

Mr. Patrick Brown: We're looking at the profile of the cyberbully, and I think there certainly are different impressions when you look at cyberbullying among youth. Could you maybe aid the committee and give us your profile of the average cyberbully, based on age and geography?

Chief Jim Chu: It's an easy question to answer. Think back to your grade 7 class and picture the bully. Now picture that same grade 7 class, anyone in the class can be the bully. That's the difference.

Mr. Patrick Brown: With no regard to gender, age, or geography...?

Chief Jim Chu: That's correct.

Whereas people before would engage in face-to-face bullying, and then you would know who they were: it could be the shyest, quietest, most respectful kid in the back of the room who has received some slight or is angry; or it could be a bunch of girls who don't like Suzie because of the way she dressed. Thos are all real examples that happen today. This is why prevention is so important. It is always why early intervention is so important, because in the majority of these cases we seem to find out who did it, but it's not going to lead to criminal charges. That would bog down the criminal justice system. We are peace officers and we're trying to prevent crime. That's our primary objective.

A/Commr Joe Oliver: The only item I would add is that given the Internet, the location could be anywhere globally, individuals may take on a persona whereby they portray themselves as a 14-year-old, they start a relationship, they get each other to exchange intimate images, then it turns out to be a predator who is now extorting more graphic images and threatening to post those images on Facebook to all their friends if they don't comply with the demands of the predator.

Mr. Patrick Brown: When you look at that one app, 700 million a day; it's phenomenal.

There's a comment from Halifax.

The Chair: Chief Blais, the floor is yours. Chief Jean-Michel Blais: Thank you.

I wanted to add to what the assistant commissioner mentioned about the geographic boundaries. We have to get out of the mindset that this can occur in the same town, in the same province, for that matter. As I spoke before about the whole notion of digital natives as opposed to digital immigrants, the young kids today have grown up with that. I have an 11-year-old boy who is considerably more articulate than I am, and able to use everything in our house from a technological point of view. His network of friends go well beyond the borders of Canada, they go into Europe and everywhere else. When you get into the anonymous aspect of what the Internet provides, and other technologies are providing as well, then it's very difficult to be able to get an idea of where people are going. It's a really important point that in the years to come, technology will increase and change, the complexity and sophistication will be even more difficult. I believe that Chief Chu was absolutely right. I would expect us to be back in a few years asking for more tools.

● (1225)

The Chair: Thank you for those questions and answers.

Our next questioner is Mr. Jacob, from the New Democratic Party. [*Translation*]

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

My thanks to our witnesses for being with us today.

My first question goes to Mr. Chu, Mr. Pardy, Mr. Oliver and Mr. Blais. I am very pleased to learn that prevention is very

important for you. As the old saying goes, an ounce of prevention is worth a pound of cure. It continues to be true in 2014.

In your respective parts of the country, what are the main programs you have established with schools and community organizations?

Mr. Chu, you can start.

[English]

Chief Jim Chu: We have strong partnership with our school boards. We have bilingual brochures that regularly go out to parents which are multilingual. We also have a partnership with a community provider, Telus Cares. That brings, again, awareness of proper protocols and safety measures you can take over the Internet.

We also refer people to several websites, NeedHelpNow.ca, and stopcyberbullying.org, many great resources as well.

A/Commr Joe Oliver: I defer to my colleague who has more intimate knowledge of prevention efforts.

Insp Mercer Armstrong (Officer in Charge of Policy and Compliance, Contract and Aboriginal Policing, Royal Canadian Mounted Police): In the RCMP across the country, community involvement and especially involvement with our youth are extremely important. Because of that we have developed a number of programs, not just within the RCMP but also in cooperation with various other organizations.

A little earlier in his introduction, Assistant Commissioner Oliver mentioned a partnership with PREVnet, Promoting Relationships and Eliminating Violence Network; and the University of Victoria with regard to the WITS program. However, that is combined with a number of other efforts that we have. Within the RCMP we have developed a curriculum that is used by our members in the classrooms of our schools across the country and is available also to those teachers in the schools. It's not only available to them; all the material that we have on cyberbullying and other types of youth issues is on our public Internet site. Not only can the RCMP use these things but also people from the public, whatever community organization they may be with. All of that material is there ready for them to use.

To give you a little bit of an idea with regard to the type of material that is there, we have self-assessment materials for young people to use. One is called "Cyberbullying-Delete it From Your Online Life!", as well as "Bullying-Has It Happened to Me?" Then we have connections to many organizations including the Red Cross and a number of other organizations. They provide excellent material that is available not only to the people who want to prevent bullying, but also the young people themselves, to get help and to point them to places where they can get help right across the country. That's just a little bit of what we've done in the RCMP.

All of our front line members are expected to be involved in the communities, and so in the contract provinces, not including Ontario and Quebec but everywhere else in the country where we are the basically the provincial police, all of our members are involved in dealing with community issues, and in the schools, and dealing with these problems.

The Chair: Mr. Pardy, do you want to speak on behalf of the

Mr. Carson Pardy: Yes. I'll try to give a broad overview of some of the programs we have in place in Ontario. First, I'll focus on the provincial strategy we have for protecting children against child abuse.

This strategy involves the partnership of 18 police services across Ontario. This strategy started in 2006 and collectively has investigated over 22,000 incidents of child sexual abuse and made countless arrests, and well over 8,000 charges and over 2,500 arrests have been made with respect to that strategy. This is about leveraging our collective input so that together as a police community we can focus on the commonalities we have from one jurisdiction to another, because as we've heard repeatedly today, this crime knows no borders. That strategy is more from an enforcement perspective.

At the community level, we have school resource officers, community services officers who are constantly in touch with the media. We view our media as one of our critical partners in delivering key safety messages right across the board; our school resource officers are working with the kids right in the schools themselves. NeedHelpNow, one amazing tool that's available, we constantly put out to the kids through posters and brochures in the hallways of our schools. This is a very intuitive website that helps direct kids and gives them very quick answers. It gives them guidance on how to tackle this.

The youthconnected ca that I mentioned earlier is a program that the OPP completely supported, along with the Ontario Provincial Police Youth Foundation and some private partners, to develop this website that was created by teenagers themselves. In that program, it gives lesson plans, for example, that teachers and parents can use to help guide and instruct children on safer Internet practices.

Annually, there's a Safer Internet Day and in those avenues we're constantly educating public displays on safe Internet. Just yesterday in the City of Brockville, there was a kiosk set up in the malls during police week, focusing on safe Internet usage and how to guide, instruct, and educate our children and our teenagers on this phenomenon of sexting, as an example.

There's a lot more going on. Our focus right now is educating our front-line officers to give good advice, that we're giving proper guidance to parents and teachers and teens themselves so that they're not misled and that they don't feel helpless, and that we are there to do our part.

On a broader sense, however, we realize that because of the economics of policing, we're having to capitalize more greatly on our partnership through our framework for action in Ontario for crime prevention, and our community mobilization and engagement of our stakeholders in our community. We alone cannot solve these problems. From an enforcement perspective, we're there. We can provide investigative excellence, but if we do not have community partners at all levels, we will not be able to fill our mandate to keep our communities safe.

(1230)

The Chair: A question was also asked of you, Chief Blais, that you may want to answer.

[Translation]

Chief Jean-Michel Blais: Mr. Jacob, like other police forces in Canada, we have liaison officers in schools and community resource officers carrying out awareness campaigns against cyberbullying. As my colleague from the Ontario provincial police pointed out, last week was national police week.

In recent years, we have seen a change in what people in shopping malls and in schools are telling us during those events. They are no longer just talking about drug crimes, but also crimes associated with cyberbullying, "sexting", and so on.

In the internal training that our police officers receive, we focus our involvement on the trauma, in order to prevent victims from being traumatized again.

We have a major presence on social media like Facebook and Twitter. We have reduced our presence on traditional websites so that we can be more present on Twitter and Facebook. I know that a number of police forces in Canada are doing the same.

In a sense, we are very lucky. At provincial level, we have the CyberSCAN unit that conducts investigations that have so-called penal, but not criminal, consequences. The province is responsible for that unit.

That is the situation here in Halifax.

● (1235)

[English]

The Chair: Merci, Chief.

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

Mr. Kyle Seeback: One of the other issues or concerns raised at the committee, and I think Mr. Fraser was talking about it, are those surrounding the definition of transmission data. He was saying that under Bill C-13, transmission data is way broader than what you get from the existing Criminal Code provisions for telephone calls.

My understanding is that when you are looking at transmission data, you're only getting the type, the date, the time, the origin, the destination, or the termination of a communication. It doesn't include the content, and you're not getting all of the metadata. That's my understanding of how it's being defined in the Code.

Does anyone want to comment on that, and let us know your view of transmission data and if it's way too broad as is being alleged? A/Commr Joe Oliver: Our understanding of transmission data—I mean, it's very clearly spelled out in the proposed legislation already. It clearly indicates that the content of transmission, which "does not reveal the substance, meaning, or purpose of the communication", is to be disclosed to police and you can't get a product order for that or use that provision to get that information. You have to rely on other means, including a general production order, which has a higher threshold.

Mr. Kyle Seeback: So if you want more information from that transmission data, what would be the process for that then?

A/Commr Joe Oliver: We would have to either secure a search warrant for the physical device and then do an analysis, or we'd have to go to the service provider with a general production order. This is for historical data.

Mr. Kyle Seeback: What's the threshold for that, then?

A/Commr Joe Oliver: For historical, a general production order is reasonable grounds to believe, so it's a higher threshold.

Mr. Kyle Seeback: And it's with judicial authorization.

A/Commr Joe Oliver: Correct. All of the provisions within the proposed legislation include prior judicial authorization. Transmission data and our understanding of how it would be applied is a modern equivalent to phone-call information in terms of the origin and the type. It includes a little bit more insofar as the size and the type, but pretty much everything else is...but the direction, the date, time, the origin, destination—those are the things we would normally get with an order for telephone information.

Mr. Kyle Seeback: Great. That's it. The Chair: Thank you very much.

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

Ms. Ève Péclet: Thank you, Mr. Chair. I'll be sharing my time with my colleague Mr. Garrison.

My question is for Mr. Oliver. One of the witnesses expressed doubt about the main section of the bill, saying that there's a challenge with it. I'm going to read out what he said, because he expressed it perfectly. He said that the real challenge arises when addressing third parties who do not know the person depicted in the image, nor do they know the circumstances under which the image was taken.

So the provisions in the bill include a recklessness standard, which is too low. How would you manage that? Do you think there should be a revisit of that proposed section, like raising the standard, because third parties could be caught in a situation where they didn't know. The proposed section states that "being reckless as to whether or not". Is the recklessness standard too low?

Mr. Chu, do you have a comment?.

Chief Jim Chu: The recklessness standard actually comes up with criminal negligence, in terms of, were you intentionally doing the act or were you reckless in doing the act? When we proceed with charges, we have to satisfy, at least in British Columbia, the charge approval standard and the reasonable likelihood of conviction. Then it's up to the judge, in terms of the factual basis of whether this reckless behaviour was inadvertent or egregious to the point where it's a criminal offence.

(1240)

Mr. Randall Garrison: Thank you very much, Mr. Chair.

There are a lot of things in Bill C-13. One is that it reopens the hate crime section of the Criminal Code to add additional identified groups. As I know, Chief Chu will be familiar, my private member's Bill C-279, which passed the House over a year ago, is either sleeping or stuck in the Senate, whichever analogy you like.

We have said that we have the intention of bringing the amendment to the committee, since that section is being opened, to add gender identity to the hate crime section of the Criminal Code, which is half my private member's bill.

I'm asking an easy question of Chief Chu. Police deal a lot with violence on the streets. Transgender people are more often subject to violence than others. I wonder whether you would see that as something we could do in this bill.

Chief Jim Chu: This is something that we would support, yes.

Mr. Randall Garrison: Are there any others who—?

Mr. Carson Pardy: I'd say the same thing.

Mr. Randall Garrison: It's been my experience that everybody who's worked in policing on the streets recognizes the higher levels of violence directed at transgendered people.

I appreciate the support of the police for that. We had an expression from the minister when he was here that he had no objection to that.

Hopefully, we'll see that added to become part of the government bill. Thank you.

The Chair: There's still some time left in this slot, and I know Mr. Jacob had another question.

Mr. Jacob.

[Translation]

Mr. Pierre Jacob: I would like to know approximately what percentage of your work, your budget, is allocated to prevention.

Let's start with Mr. Chu and then move to Mr. Armstrong, Mr. Pardy and Mr. Blais.

[English]

The Chair: He wants an answer from all four witness groups.

[Translation]

Mr. Pierre Jacob: I want to know what the approximate percentage is.

[English]

Chief Jim Chu: A large part of every police officer's job is a game of crime prevention. It's hard to break it out. A front-line officer will take a call, and then while taking the police report they will speak with the victim about preventative measures. Even with our school liaison officers, a large portion of their work is preventative, but of course they're also involved in investigating crime at the same time.

It's a primary focus of policing across Canada. A major portion of our job is prevention.

[Translation]

Mr. Pierre Jacob: Can we say that it is about 25%? [*English*]

The Chair: Do you want to guess?

OPP, do you have a guess?

Mr. Carson Pardy: I would have to say that everything that we do, from enforcement to lecturing kids in school, is a form of prevention. It would be very, very difficult to quantify.

We have focused specific officers through a school resource program, through our community services officers, through our youth issues unit, and our liaison with the media, but to actually quantify it...I would say 100%.

The Chair: Chief Blais, do you have any additional comments to that question?

[Translation]

Mr. Pierre Jacob: Go ahead, Mr. Blais.

Chief Jean-Michel Blais: It is a little hard to quantify. Mr. Pardy was not wrong when he said that, in a way, preventing crime is 100% of our work. I think it was you who said that prevention is of great value in criminal matters. It is just like a disease, when you can prevent it, you do. In every police force, officers are assigned to prevention in every sense of the word. In terms of numbers, funds are allocated for it, of course; it is at least 10% of our resources. So, whatever the case, it can vary between 10% and 100%.

Mr. Pierre Jacob: Thank you very much.

[English]

The Chair: And the last comment will be from our RCMP friends.

Insp Mercer Armstrong: In terms of cost, we can certainly cost programs that are financed to deal with prevention. But when it comes to the person costs, I have to agree with the other speakers: for all of our members, the mindset is to be involved in prevention. What they do in dealing with the community is geared towards prevention. Of course, there are the specific programs that they're involved in and the specific actions they take to head off issues in the communities, but that's all part of what they do. So I would go with 100% also.

● (1245)

The Chair: Thank you very much.

I want to thank our witnesses for joining us today. It was very informative and we had very good answers to the questions.

As you know, there's a break week and we'll be back in the ridings. Then we'll be back at this probably until mid-June, when we'll hopefully be doing clause by clause back in the House. If you're interested in keeping track of how this bill is going, that is about the timeframe before this committee will deal with it.

Before the committee goes, we do have a budget for witnesses that I need approved. There are a number of witnesses who have been before us, and more to come. It's for about \$18,000. My clerk says that's more than we normally need, but he wants to be safe just because we don't know where they're coming from.

Would somebody move that for me?

Mr. Bob Dechert: I so move.

(Motion agreed to)

The Chair: Thank you very much.

Thank you for joining us.

This meeting is adjourned.

Published under the authority of the Speaker of the House of Commons

SPEAKER'S PERMISSION

Reproduction of the proceedings of the House of Commons and its Committees, in whole or in part and in any medium, is hereby permitted provided that the reproduction is accurate and is not presented as official. This permission does not extend to reproduction, distribution or use for commercial purpose of financial gain. Reproduction or use outside this permission or without authorization may be treated as copyright infringement in accordance with the *Copyright Act*. Authorization may be obtained on written application to the Office of the Speaker of the House of Commons.

Reproduction in accordance with this permission does not constitute publication under the authority of the House of Commons. The absolute privilege that applies to the proceedings of the House of Commons does not extend to these permitted reproductions. Where a reproduction includes briefs to a Committee of the House of Commons, authorization for reproduction may be required from the authors in accordance with the *Copyright Act*.

Nothing in this permission abrogates or derogates from the privileges, powers, immunities and rights of the House of Commons and its Committees. For greater certainty, this permission does not affect the prohibition against impeaching or questioning the proceedings of the House of Commons in courts or otherwise. The House of Commons retains the right and privilege to find users in contempt of Parliament if a reproduction or use is not in accordance with this permission.

Publié en conformité de l'autorité du Président de la Chambre des communes

PERMISSION DU PRÉSIDENT

Il est permis de reproduire les délibérations de la Chambre et de ses comités, en tout ou en partie, sur n'importe quel support, pourvu que la reproduction soit exacte et qu'elle ne soit pas présentée comme version officielle. Il n'est toutefois pas permis de reproduire, de distribuer ou d'utiliser les délibérations à des fins commerciales visant la réalisation d'un profit financier. Toute reproduction ou utilisation non permise ou non formellement autorisée peut être considérée comme une violation du droit d'auteur aux termes de la *Loi sur le droit d'auteur*. Une autorisation formelle peut être obtenue sur présentation d'une demande écrite au Bureau du Président de la Chambre.

La reproduction conforme à la présente permission ne constitue pas une publication sous l'autorité de la Chambre. Le privilège absolu qui s'applique aux délibérations de la Chambre ne s'étend pas aux reproductions permises. Lorsqu'une reproduction comprend des mémoires présentés à un comité de la Chambre, il peut être nécessaire d'obtenir de leurs auteurs l'autorisation de les reproduire, conformément à la Loi sur le droit d'auteur.

La présente permission ne porte pas atteinte aux privilèges, pouvoirs, immunités et droits de la Chambre et de ses comités. Il est entendu que cette permission ne touche pas l'interdiction de contester ou de mettre en cause les délibérations de la Chambre devant les tribunaux ou autrement. La Chambre conserve le droit et le privilège de déclarer l'utilisateur coupable d'outrage au Parlement lorsque la reproduction ou l'utilisation n'est pas conforme à la présente permission.

Also available on the Parliament of Canada Web Site at the following address: http://www.parl.gc.ca

Aussi disponible sur le site Web du Parlement du Canada à l'adresse suivante : http://www.parl.gc.ca