THE CANADIAN BAR ASSOCIATION
L'ASSOCIATION DU BARREAU CANADIEN

Bill C-13, *Protecting Canadians from Online Crime Act*

CANADIAN BAR ASSOCIATION

May 2014

500-865 Carling Avenue, Ottawa, ON, Canada K1S 5S8
tel/tél : 613.237.2925 | **toll free/sans frais** : 1.800.267.8860 | **fax/téléc :** 613.237.0185 | info@cba.org | **www.cba.org**

PREFACE

The Canadian Bar Association is a national association representing 37,500 jurists, including lawyers, notaries, law teachers and students across Canada. The Association's primary objectives include improvement in the law and in the administration of justice.

This submission was prepared by the National Criminal Justice, with input from the Privacy Law and Competition Law Sections, and the Children's Law Committee of the Canadian Bar Association, and with assistance from the Legislation and Law Reform Directorate at the National Office. The submission has been reviewed by the Legislation and Law Reform Committee and approved as a public statement of the Canadian Bar Association.

TABLE OF CONTENTS

Bill C-13, *Protecting Canadians from Online Crime Act*

I. INTRODUCTION 1

II. CYBERBULLYING OFFENCE 2

A. Addressing the Gap 2
B. "Publishes, distributes, transmits, sells, makes available or advertises" 4
C. Recklessness and Knowledge Regarding Consent 6
D. Neutral Platform Providers 8
E. Sentencing 9
F. Conclusion 10

III. LAWFUL ACCESS 11

A. Introduction: Privacy and Law Enforcement 11
B. Preservation Demands and Orders 13
C. Production Orders 17
D. Tracking Warrants and Data Recorder Warrants 21
E. Conclusion 23

IV. *COMPETITION ACT* AMENDMENTS 24

V. CONCLUSION 25

Bill C-13, *Protecting Canadians from Online Crime Act*

I. INTRODUCTION

The Canadian Bar Association's National Criminal Justice Section, with input from the CBA's Privacy Law and Competition Law Sections, and the Children's Law Committee (CBA), is pleased to comment on Bill C-13, *Protecting Canadians from Online Crime Act*. The CBA recognizes the need to address how the Internet can be used by some to harass, intimidate and threaten others, especially vulnerable children,[1] an activity now referred to as cyberbullying. We support the government's efforts to fill an obvious legislative "gap" with Bill C-13, and offer our recommendations to improve the Bill.

Bill C-13 would criminalize cyberbullying, which has become an increasingly pressing problem following a rash of recent and tragic cases involving young people bullied online. The tragic suicides of Rehtaeh Parsons and Amanda Todd, among others, have sparked a national debate.

When introducing Bill C-13, the Honourable Peter MacKay, Minister of Justice and Attorney General of Canada, stated:

> Our government is committed to ensuring that our children are safe from online predators and from online exploitation. We have an obligation to help put an end to harmful online harassment and exploitation. Cyberbullying goes far beyond schoolyard bullying and, in some cases, can cross the line into criminal activity.[2]

The CBA supports the goal of protecting children from cyberbullying. However, the mechanism used to meet that goal – creating a new criminal offence – must be drafted with precision to

---

1 In this submission, we use the terms 'child' and 'children' to refer to people under the age of 18 who have particular legal rights under the *UN Convention on the Rights of the Child*, ratified by Canada in 1991. 'Young person' and 'young people' refer more specifically to people between the ages of 12 and 17, who can be subject to prosecution under the *Youth Criminal Justice Act*.

2 Department of Justice, "Government Introduces Legislation to Crack Down on Cyberbullying", www.justice.gc.ca/eng/news-nouv/nr-cp/2013/doc_32994.html.

capture only the impugned conduct. To that end, we recommend specific amendments to the offence provision.

Bill C-13 goes far beyond cyberbullying to revisit general provisions for the search and seizure of Internet data, referred to as "lawful access" legislation. The proposals in Bill C-13 are more focused and circumscribed than previous legislative initiatives, and we believe that with our recommended amendments would produce a viable version of this important legislation. Updated provisions for the search and seizure of Internet data are essential for the exercise of substantive criminal law provisions like the new cyberbullying offence.

However, previous lawful access legislation has been very controversial, and including lawful access in Bill C-13 has the potential to detract from the focus on cyberbullying. For the protection of children and young people to receive appropriate attention, the CBA suggests dividing Bill C-13 into two separate bills, one for cyberbullying and one for lawful access.

RECOMMENDATION:

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

II. CYBERBULLYING OFFENCE

A. Addressing the Gap

Bill C-13 would introduce a hybrid offence aimed at criminalizing the publication of intimate images without consent:

> 162.1 (1) Everyone who knowingly publishes, distributes, transmits, sells, makes available or advertises an intimate image of a person knowing that the person depicted in the image did not give their consent to that conduct, or being reckless as to whether or not that person gave their consent to that conduct, is guilty…

"Intimate image" is defined in subsection (2) as:

> …a visual recording of a person made by any means including a photographic, film or video recording,
>
> (a) in which the person is nude, is exposing his or her genital organs or anal region or her breasts or is engaged in explicit sexual activity;

> (b) in respect of which, at the time of the recording, there were circumstances that gave rise to a reasonable expectation of privacy; and
>
> (c) in respect of which the person depicted retains a reasonable expectation of privacy at the time the offence is committed.

If prosecuted by way of indictment, an accused is liable to imprisonment for a term of not more than five years.

As Minister MacKay's comments illustrate, Bill C-13 is primarily intended to protect children and youth from online predators and exploitation. However, existing *Criminal Code* provisions already criminalize the dissemination of sexual depictions of children (see section 163.1 – Child Pornography). In fact, the language of the proposed cyberbullying offence mirrors the child pornography offences in the *Criminal Code* and the existing offences provide greater protection than Bill C-13 would, as they criminalize mere possession of such images.

Given this, the real change and expansion of criminal powers in Bill C-13 concerns the unlawful use of "intimate images" involving adults. Currently prosecutors must use offence provisions that were created before cyberbullying existed, such as the criminal harassment offence. Rather than increasing the protection of children and youth, this is the area in which Bill C-13 actually addresses a current gap in Canada's legislative scheme.

Under proposed section 162.1(1), individuals who publish, distribute, transmit, sell, advertise or make available intimate images of adults without consent could be charged. Given the serious harm this conduct may cause, the CBA welcomes this addition to the *Criminal Code*, again subject to recommended refinements below.

While Bill C-13 does not actually enhance protection of children and youth who are *victims* of cyberbullying, the proposed offence would offer prosecutors an important alternative when dealing with people under 18 alleged to have disseminated intimate images of other youth. The Bill provides a more moderate option for prosecuting youths who disseminate intimate images of their peers without consent than the existing child pornography provisions, which are harsher both in penalty and associated stigma.

Cyberbullying is clearly a serious issue for children and youth in Canada. However, the criminal law should be considered a tool of last resort when dealing with young offenders, and not all incidents of cyberbullying by youths should be characterized as criminal acts. For most

youthful perpetrators, an educational or diversionary response is more appropriate.[3] It is also important to recognize that youths are often not only victims, but may themselves be 'cyberbullies' or 'bystanders' at other points in time. This must be carefully considered in assessing what is truly in the best interests of all Canadian children, as these roles may shift from one interaction to the next.

B. "Publishes, distributes, transmits, sells, makes available or advertises"

Proposed section 162.1 would capture various types of cyberbullying conduct, criminalizing some acts that are not currently prohibited, and again, including other acts already covered as child pornography in section 163.1 of the *Criminal Code*. It would criminalize any dissemination of intimate images without the depicted person's consent. However, the section is drafted to apply also to conduct that would not generally be considered cyberbullying.

The Backgrounder, Press Release and Ministerial comments about Bill C-13 all suggest this legislation will combat the illegal distribution of intimate images for the purpose of bullying individuals depicted in the images. Bullying can take many forms, including harassment, embarrassment, annoyance and intimidation. Bullying is deliberate. While we assume that the proposed legislation is not intended to target inadvertent or careless distribution of images, without the necessary motive or intent, the current wording of section 162.1 could have that effect.[4]

While the cyberbullying provisions are expressly aimed at criminalizing conduct where there is a malicious intent, they would actually capture conduct without any such intent. The proposed wording of section 162.1 is consistent with a privacy-based offence, as recommended by the Coordinating Committee of Senior Officials (CCSO) Cybercrime Working Group.[5] However, the stated legislative intent of Bill C-13 is to criminalize cyberbullying, defined as the "use of

---

3 For a useful discussion about existing alternative, non-criminal measures adopted to combat cyberbullying, please see: CCSO Cybercrime Working Group, "Report to the Federal/Provincial/ Territorial Ministers Responsible for Justice and Public Safety: Cyberbullying and the Non-consensual Distribution of Intimate Images", June 2013 [CCSO Cybercrime Working Group] at 6-8.

4 It is not uncommon for youth to take sexually explicit photographs of themselves to share with other youth who, in turn, may distribute the images without consent. Prosecuting youth for child pornography offences in these circumstances arguably goes beyond the intent of section 163.1 (see *R. v. Sharpe*, [2001] 1 S.C.R. 45). There is an ongoing constitutional challenge to the child pornography provisions as applied to youths in similar circumstances. This illustrates the importance of limiting the new cyberbullying offence to non-consensual distribution of intimate images.

5 *Supra*, note 3.

information and communication technologies that support deliberate, hostile and often repeated behaviour by an individual or group that *is intended to hurt others*."[6] The CBA believes that the wording of the section should be refined to accord with its stated purpose.

For example, "makes available" in the proposed section 162.1 creates possibilities of criminal liability well beyond what reasonable Canadians would consider to be cyberbullying. Consider the following:

> Mr. Smith lends his laptop to a friend, Mr. Jones, to browse the Internet while his cable is being fixed. Mr. Smith knows that the computer contains two intimate images of himself and his wife, but they are deep within a folder labeled "Private". Mr. Smith also knows that his wife expects those images to remain private. He trusts Mr. Jones will not scour the computer looking through each folder.
>
> However, Mr. Jones gets bored with browsing, and begins to randomly open folders – ultimately discovering the two intimate images. At the same time, a visitor in his home, also an acquaintance of Mr. Smith's wife, walks by and sees the image. Disturbed, she informs the police and the computer is seized.

In this example, Mr. Smith has no intention of bullying his wife by lending his laptop to his friend. Under Bill C-13, he could be convicted of "making an intimate image available without consent", as he intentionally made his computer available to Mr. Jones knowing both that intimate images were in the computer and that his wife did not consent to sharing those images.

Other examples where a person could have made intimate images available without intending to bully anyone depicted in the images are easy to imagine. Individuals can hyperlink to virtually anything on the Internet, and their capacity to "make available" images is endless.

Bill C-13 could also have an impact on the media. It appears that photojournalists who publish images of celebrities or politicians in compromising situations could be subject to criminal sanction under the proposed legislation.[7]

Simple additions to section 162.1 could fix this problem, and narrow the scope to the conduct Parliament apparently contemplates – the intentional bullying of others by dissemination of intimate images.

---

6 *Ibid.* at 3.

7 A defence of "public good" is included in the proposed legislation which may cover some of the media's potential criminal exposure.

RECOMMENDATION:

2. **The Canadian Bar Association recommends that section 162.1(1) be amended to include the words "with the intent to annoy, embarrass, intimidate or harass that person".**

3. **The Canadian Bar Association recommends that the following be added to section 162.1: "No person shall be convicted of an offence under this section if the distribution, transmission, selling, making available or advertising that forms the subject-matter of the charge is for the public's information or is a matter of public interest."**

C. Recklessness and Knowledge Regarding Consent

If a person takes or receives an intimate image directly from someone they know personally, it might be easy to determine whether consent was given to further share the intimate image. However, laptops, smartphones and other electronic devices facilitate sharing and re-sharing intimate images multiple times in just seconds. This suggests a sliding scale of moral culpability and a wide range of people who could potentially be accused of the proposed offence, some with little or no knowledge of the person depicted in the image.

Including "recklessness" in the proposed offence raises the question of whether someone must take steps to ascertain consent before sharing an image, even when they do not know the person depicted or how the image was obtained. There will often be no means or ability to ascertain consent in such circumstances.

Again, the aim of the proposed provision is to criminalize the sharing of an image with intent to bully someone who appears in the image. If an individual distributes an intimate image without any knowledge of where it came from or who is depicted, there is no intent to bully the person depicted in the image. However, as currently worded, the individual sharing the image could be subject to criminal sanction if reckless as to whether or not consent was obtained.

Removing the recklessness standard from the proposed offence would restore the intended focus on conduct that actually constitutes cyberbullying. This reflects the critical distinction between provisions which actually aim to combat bullying, rather than aimed purely at protecting privacy.

The proposed section 162.2 should rest on the term "knowingly." In criminal law, the concept of knowledge includes the concept of "willful blindness". A standard of willful blindness captures perpetrators who become aware of the need for enquiry regarding consent, but decline to make that enquiry (because they do not wish to know if consent was given).[8] In other words, without the recklessness standard, an accused still may be guilty if he or she suspected non-consent and purposefully turned a blind eye to that issue before sharing the intimate image.

In the previous example, if Mr. Jones subsequently copied the intimate images he found and emailed them to another friend (Mr. Johnson), he would be liable under section 162.1, even though he did not personally take the photographs and did not ask Mr. Smith about them. Due to the nature of the images, Mr. Jones' knowledge of who was depicted, and the fact that he found the images within several folders, in one labeled "Private", arguably he was willfully blind to the issue of consent.

But, imagine that Mr. Johnson received the unexpected and shocking images on his phone while standing next to a friend, and turned to show his friend what he had just received. He did not know who appeared in the images, where they were taken, or the name of the folder in which they had been found. Still, if Mr. Johnson knew there was a risk that the people in the images had not consented to distribution (for instance, because of the amateurish nature of the photography[9]), he might be considered reckless regarding consent when he instinctively reacted by turning to show his friend. Under Bill C-13 now, Mr. Johnson could be criminally liable without intending to bully Mr. Smith's wife (or Mr. Smith.). Mr. Johnson's "distribution" of the images (when he turned to show his friend his phone) does not seem to be the conduct that Bill C-13 intends to criminalize.

RECOMMENDATION:

4. **The Canadian Bar Association recommends that section 162.1(1) be amended to remove the words "or being reckless as to whether or not that person gave their consent to that conduct".**

---

8 *R. v. Sansregret*, [1985] 1 S.C.R. 570.

9 On the other hand, if a photo is not amateurish, but appears professionally taken, a recipient may reasonably assume that the model is a professional and not consider any issue of consent or bullying. Prosecution for distribution should not depend on obvious deficiencies in a photo, the quality of the camera, etc.

D. Neutral Platform Providers

Bill C-13 could criminalize Internet platforms designed for lawfully sharing content, consistent with "terms of use", "community standards" or other rules of good conduct. In spite of such precautions, neutral platform providers can be unwittingly misused for cyberbullying.

Online service providers have no knowledge of material stored on their platforms or what is shared with other users, and should not be exposed to criminal liability because of their users' conduct unless they are equally culpable. For example, certain social media websites permit a user to "share" an image with a small group of users or the public at large. The website provider may be unable to pre-screen images and would have no knowledge of whether a person in an image had consented to dissemination of the image. Telecommunications companies that provide text-messaging or video-messaging services are in the same position. If culpability is based on "recklessness", importing an obligation to make due enquiries, platform providers will likely be unable to identify and contact persons who appear in images to enquire as to consent.

Another type of neutral service provider is a search engine that indexes content available on other websites and services and produces results in response to queries. The operators of search engines do not know of the circumstances in which indexed images or videos were produced, or whether persons have consented to dissemination. There may be no way to determine this information from the images or surrounding data.

Some online organizations exist for the purpose of disseminating intimate images without consent of the individuals depicted. These organizations are properly within the ambit of the proposed legislation. But exposing neutral service providers to criminal liability is unreasonable and unlikely to survive *Charter* scrutiny due to the absence of moral culpability, which is required for criminal sanctions.

RECOMMENDATION:

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

E. Sentencing

A maximum five year penalty is an appropriate range of sanction for the proposed section 162.1 offence. That maximum penalty accords with similar provisions in the *Criminal Code*, and allows Canadian judges to dispose of this offence by way of conditional discharge or conditional sentence in appropriate circumstances.

Bill C-13 also would amend the restitution provision of the *Criminal Code*, adding the following subsection:

> 738(1)(e) in the case of an offence under subsection 162.1(1), by paying to a person who, as a result of the offence, incurs expenses to remove the intimate image from the Internet or other digital network, an amount that is not more than the amount of those expenses, to the extent that they are reasonable, if they amount is readily ascertainable.

The CBA considers this a logical and welcome change as it aims to compensate victims for direct costs incurred as a result of criminal cyberbullying.

Finally, a new prohibition order is proposed in Bill C-13 under section 162.2:

> 162.2(1) When an offender is convicted, or is discharged on the conditions prescribed in a probation order under section 730, of an offence referred to in subsection 162.1(1), the court that sentences or discharges the offender, in addition to any other punishment that may be imposed for that offence or any other condition prescribed in the order of discharge, may make, subject to the conditions or exemptions that the court directs, an order prohibiting the offender from using the Internet or other digital network, unless the offender does so in accordance with conditions set by the court.
>
> (2) The prohibition may be for any period that the court considers appropriate, including any period to which the offender is sentenced to imprisonment.

Subsection (3) allows for an application to vary an order made pursuant to section 162.2(1). Subsection (4) makes it an offence to fail to comply with an order made pursuant to section 162.2(1). Certainly, in some circumstances, it may be appropriate to prohibit an offender from accessing the Internet for a period. However, section 162.2(2) should be reasonable and limited to a maximum of five years. As drafted, the Bill would allow a court to prohibit someone from using the Internet for life. Given the prevalence of the Internet in the day-to-day workings of society, this could be devastating and constitute a disproportionate sanction.

A person prohibited from accessing the Internet may not be able to apply for employment online (an increasingly common method of recruiting), pay bills online, file tax returns online or do many other essential tasks that increasingly are limited to the Internet. Young people prohibited from accessing the Internet may be prevented from participating in regular school assignments and activities, and so may be impeded in completing their education. The current wording of section 162.2(1) includes the phrase "unless the offender does so in accordance with conditions set by the court", but the section seems to permit a court to prohibit the accused from accessing the Internet without any exceptions.

RECOMMENDATION:

6. **The Canadian Bar Association recommends that section 162.2 be amended by requiring the court to provide the offender with (an) exception(s) to any prohibition ordered pursuant to section 162.2(1).**
7. **The Canadian Bar Association recommends that section 162.2(2) be amended to require a reasonable prohibition, with a maximum Internet prohibition of five years.**

F. Conclusion

Any legislative response to the broad social problem of bullying should be accompanied by a strong focus on education and prevention so that young people – be they potential or actual bullies, victims or bystanders – understand the social, health and legal consequences of their digital actions for themselves and others. Young people can best protect themselves and others, and adapt their own behaviour, when they are effectively informed about the risks and have tools to respond to unwanted emails, texts and images.

Youth are not only more impulsive because of their developmental stage, but they think less about the future than adults. Short-term interests are likely to outweigh the seemingly remote possibility of legal consequences. Overemphasis on penalties, rather than prevention and education, misses the point at which behaviour should be addressed – that is, before someone impulsively takes a photo or hits the "send" button. Only the most serious of cases should result in criminal charges against youth. And, there should be careful ongoing analysis and evaluation of both intended and unintended impacts of this proposed legislation.

In UNICEF's recent "report card" on child well-being, Canada ranked 21st of 29 industrialized nations in the incidence of bullying.[10] Canadians should consider how better-ranked countries like Italy, Sweden and Spain are preventing harm, loss and senseless deaths. Ultimately, there is no "quick fix" for cyberbullying and the harm it causes – even where criminal law sanctions are invoked. What can make a significant difference is a heightened sense of collective responsibility, with parents, teachers, social workers, health professionals, law-enforcement officials, policymakers and the private sector, together with young people, all assuming a greater role in effective prevention and sensitive communication.

III. LAWFUL ACCESS

A. Introduction: Privacy and Law Enforcement

The CBA has commented on several lawful access proposals over the past twelve years. In 2002, the CBA responded to the federal government's initial public consultation about lawful access. In 2005, we responded to a more detailed consultation document. In 2006, we wrote to the federal Ministers of Public Safety and Justice, expressing concern that Internet service providers were responding to law enforcement requests without specific legislative authorization. ISP responses continue under the authority of PIPEDA and other legislation: recently it was reported that between April 2012 and March 2013, the Canada Border Services Agency requested Internet subscriber information 18,849 times. Ninety-nine percent of those requests were without judicial authorizations, and companies provided information in all but 25 cases.[11] More recently we have been prepared to respond to a number of incarnations of lawful access bills,[12] which ultimately died on the Order Paper or were withdrawn by Parliament.

The issue of obtaining subscriber identification without a warrant is currently reserved for decision by the Supreme Court of Canada in *R. v. Spencer*.[13] With the amendments the CBA proposes in this submission, we believe the remaining lawful access provisions constitute a viable attempt to make the search and seizure provisions of the *Criminal Code* functional within current technology. Data and Internet communications are routinely part of the evidence in serious criminal cases, ranging from murder to investment fraud, as well as in proposed

10 www.unicef.org/policyanalysis/index_68637.html

11 Paul McLeod, "Ottawa has been spying on you" (Chronicle Herald, March 29 2014).

12 For example, Bill C-51, *Investigative Powers for the 21st Century Act* (2010).

13 2011 SKCA 144, Supreme Court of Canada file 34644.

cyberbullying prosecutions. However, Canadians are understandably concerned because they are unable to determine what information law enforcement agencies possess about them, how it was obtained, or the purposes for which it may be used.

While this situation should be addressed, the *Criminal Code* does not, nor should it, address broad privacy concerns. Instead, the *Code* provides for the investigation and prosecution of offences, including the seizure and admissibility of data in criminal cases. In that context, an accused has standing to argue that data seized in violation of section of 8 of the *Charter* should be excluded from evidence. However, criminal proceedings do not address the privacy interests of people whose information is obtained by law enforcement agencies during investigations that do not result in criminal charges, nor does it address the privacy interests of people whose information is obtained by police because they had incidental, innocent contact with someone who may be charged with an offence.

The retention and use of personal information by law enforcement agencies is governed by the various federal and provincial privacy and document disposal acts. Long-term retention of investigative information is crucial to the resolution of "cold cases" (usually, homicides and sexual assaults) and to the investigation of ongoing criminal organization offences. Disclosure of police information imperils those investigations. Long-term retention of investigative information is also crucial to the resolution of claims of wrongful conviction.

Government is justifiably concerned about the efficacy of criminal investigations in the age of electronic data, but enhanced state power infringing on privacy must be accompanied by effective oversight mechanisms. The cumulative impact of various laws and state actions on individual privacy must be monitored to maintain the balance between effective law enforcement and the rights of individuals.

RECOMMENDATION:

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

B. Preservation Demands and Orders

Preservation Demand for Computer Data (section 487.012)

The proposed section 487.012 would provide that a peace or public officer (officer), without prior judicial authorization, may make a preservation demand. That demand would require a person to preserve computer data in their possession or control for a period of up to 21 days.

An officer would be empowered to make a preservation demand based on reasonable grounds to suspect that:

- an offence has been or will be committed under any Act of Parliament or under "a law of a foreign state," if a person or authority of the foreign state is investigating the offence; and
- the data will assist in investigation of the offence.

The demand would expire after 21 days for a suspected Canadian offence or after 90 days if a foreign offence is being investigated, unless the officer revokes the demand earlier. The officer cannot make another demand for preservation of the same data.[14]

Further, proposed section 487.0194 provides that as soon as feasible after a preservation demand expires or is revoked, the person in possession or control of the data shall destroy the data that would not be retained in the ordinary course of business – unless the "preserved" data has become the subject of a subsequent order under any of sections 487.13-487.17 (see below). "Preserved" data also shall be destroyed after a copy of it is seized under a warrant (section 487.0194(4).)

Section 487.012 (preservation demand for computer data) appears intended to preserve data without examining it. The preservation demand power is balanced by a provision that once the demand expires, data must be destroyed if it would not be retained in the ordinary course of business.

As noted in the discussion of several following sections of the Bill, the proposed threshold of "reasonable grounds to suspect" already exists in the current section 492.013 (production order for information identifying account-holders) and section 492.1 (warrant for tracking

14 Proposed section 487.012(6).

device). The threshold of "reasonable suspicion" has been considered by the Supreme Court of Canada for other types of investigation.[15]

While there may be circumstances where it is impossible to obtain judicial authorization soon enough to preserve computer data, those circumstances are the exception. In our view, if it is impractical for an officer to obtain prior judicial authorization, the warrantless demand to preserve data should have force only long enough to permit the officer a reasonable opportunity to apply for judicial authorization - a much shorter period than the 21 days proposed by section 487.012(4).

RECOMMENDATION:

9. The Canadian Bar Association recommends that officers be granted power to make a preservation demand only in exigent circumstances where there is reason to believe that the data in question may be lost or destroyed before a judicial authorization can be obtained. In those limited circumstances, a preservation demand should apply only for the time reasonably necessary to apply for judicial authorization.

Section 487.012 is drafted to make a preservation demand available on reasonable suspicion of an offence under any Act of Parliament or in relation to an offence that "has been committed under a law of a foreign state." This would make a preservation demand available for any foreign offence, criminal or regulatory, without regard to the seriousness of the offence or whether the activity would be criminal in Canada. While cooperation between countries for law enforcement purposes is important, preservation demands should be restricted to criminal offences under Acts of Parliament and criminal offences under the laws of foreign states that would also be crimes in Canada.

RECOMMENDATION:

10. The Canadian Bar Association recommends that if officers are granted power to make a preservation demand, that power be restricted to circumstances where an officer has reasonable grounds to suspect a

15 *R. v. Chehil*, 2013 SCC 48; R. v. MacKenzie, 2013 SCC 50.

criminal offence under an Act of Parliament, or a criminal offence under the law of a foreign state that would also be a crime in Canada.

Section 487.012 does not require an officer to produce or maintain a record of the grounds supporting a preservation demand. Accountability, transparency and oversight should always be the necessary companions of extraordinary state powers. Without a written record setting out the basis upon which an officer made a demand, maintaining those fundamental safeguards is impossible.

RECOMMENDATION:

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

Subsection (5) of section 487.012 would give officers power to impose unlimited conditions on preservation demands:

> (5) The peace officer or public officer who makes the demand may impose any conditions in the demand that they consider appropriate — including conditions prohibiting the disclosure of its existence or some or all of its contents — and may revoke a condition at any time by notice given to the person.

In our view, it is inappropriate and unjustified to grant officers unfettered discretion, particularly where violation of officer-imposed conditions constitutes a criminal offence. The conditions could prevent a party from exercising lawful rights, without any mechanism for judicial review or oversight. If a "gag order" is justifiable in any circumstances, it should be imposed by a court of competent jurisdiction and not by an officer with unfettered discretion.

RECOMMENDATION:

12. The Canadian Bar Association recommends that subsection 487.012(5) be omitted from Bill C-13.

Preservation Order for Computer Data (section 487.013)

Proposed section 487.013 would provide that a justice or judge, on *ex parte* application by an officer, may make a preservation order – an order that requires a person to preserve computer data in their possession or control for up to 90 days. A judge would be empowered to make a preservation order if satisfied that there are reasonable grounds to suspect that:

- an offence has been or will be committed under any Act of Parliament or under a law of a foreign state, if a person or authority of the foreign state is investigating the offence;
- the data is in the person's possession or control;
- the data will assist in investigation of the offence; and
- the judge also is satisfied that the officer intends to apply or has applied for a warrant or an order to obtain a document that contains the computer data (the Bill defines "document" as "a medium on which data is registered or marked").

The proposed preservation order would expire 90 days after it is made, for both Canadian and foreign investigations, unless revoked earlier. As soon as feasible after a preservation order expires or is revoked, the person in possession or control of the data shall destroy the data that would not be retained in the ordinary course of business – unless the data has become the subject of a new preservation order or a production order under any of sections 487.14 – 487.17 (see below). "Preserved" data also shall be destroyed after a copy of it is seized under a warrant (section 487.0194(4).)

This provision appears intended to preserve data without examining it. The preservation order is balanced by the provision that once the order has expired, data must be destroyed if it would not be retained in the ordinary course of business – however, it appears that the same data may be subject to consecutive judicial preservation orders.

As above, the threshold of "reasonable grounds to suspect" currently exists and has been considered by the Supreme Court of Canada for other types of investigation.

Section 487.012 is drafted to make a preservation order available on reasonable suspicion of an offence under any Act of Parliament or for an offence that "has been committed under a law of a foreign state." This would make a preservation order available for any foreign offence,

criminal or regulatory, again without regard to the seriousness of the offence, or whether the activity would be criminal in Canada.

The CBA recommends that the proposed preservation order under section 487.012 be restricted to criminal offences under Acts of Parliament and criminal offences under the laws of foreign states that would also be crimes in Canada.

RECOMMENDATION:

13. The Canadian Bar Association recommends that judicial preservation orders be restricted to circumstances were the judge or justice is satisfied that there are reasonable grounds to suspect a criminal offence under an Act of Parliament, or a criminal offence under the law of a foreign state that would also be a crime in Canada.

C. Production Orders

General Production Order for Documents or Data (section 487.014)

This is a renumbered revision of the well-worn section 487.012. The proposed revision clarifies the former wording, arguably raising the threshold for production orders. Under the existing section, a judge must be satisfied that there are reasonable grounds to believe that an offence "has been or is suspected to have been committed"; under the proposed section 487.014, a judge must be satisfied that there are reasonable grounds to believe that an offence "has been or will be committed."

Production Order to Trace Specified Communications (section 487.015)

New section 487.015 would provide that a justice or judge, on *ex parte* application by an officer for the purpose of identifying a device or person involved in transmitting a communication, may order a person (presumably a service provider) to prepare and produce a document containing transmission data related to identifying a device or person involved in transmitting a communication. The provision cannot be used to identify a person who is under investigation for offences (section 487.015(5)).

A judge would be empowered to make the production order if satisfied of reasonable grounds to suspect that:

- an offence has been or will be committed under any Act of Parliament;
- the identification of a device or person involved in the transmission of a communication will assist in the investigation of the offence; and
- transmission data that is in the possession or control of one or more persons whose identity is unknown will enable that identification

The officer must provide a written report to the judge who makes the production order as soon as feasible after the person from whom the communication originated is identified (section 487.015(6)). A person subject to a section 487.015 production order to trace a specified communication, with respect to data previously preserved under a preservation demand (section 487.012) or a preservation order (section 487.013), shall destroy data that would not be retained in the ordinary course of business as soon as feasible after production is made under the section 487.015 order, or as soon as feasible after the order is revoked.

This provision appears to concern the identification of "innocent hosts" such as public Wi-Fi networks. Again, the threshold of "reasonable grounds to suspect" already appears in current sections 487.013 and 492.1, and has been considered by the Supreme Court of Canada for other types of investigation.

Production Order for Transmission Data (section 487.016)

New section 487.016 proposes that a justice or judge on *ex parte* application by an officer may order a third party (a service provider) to produce transmission data. A judge would be empowered to make such a production order if satisfied that there are reasonable grounds to suspect that:

- an offence has been or will be committed under any Act of Parliament; and
- transmission data that is in a person's possession or control will assist in investigation of the offence

A person subject to a section 487.016 production order with respect to data previously preserved under a preservation demand (section 487.012) or a preservation order (section

487.013), shall destroy the data that would not be retained in the ordinary course of business as soon as feasible after production is made under the section 487.016 order, or as soon as feasible after the order is revoked. The threshold of "reasonable grounds to suspect" already appears in sections 487.013 and 492.1. However, as explained in section D below, "transmission data" may reveal "core biographical information" protected from search and seizure under section 8 of the *Charter*, so the higher threshold of "reasonable grounds to believe" should be applied in the proposed section 487.016.

RECOMMENDATION:

14. The Canadian Bar Association recommends that as "transmission data" may reveal core biographical information protected from search and seizure under section 8 of the *Charter*, the threshold of "reasonable grounds to believe" should apply in proposed section 487.016.

Production Order for Tracking Data (section 487.017)

New section 487.017 proposes that a justice or judge, on *ex parte* application by an officer, may order a third party to produce tracking data (for example, GPS data in the possession of a car rental agency.) A judge would be empowered to make an order if satisfied that there are reasonable grounds to suspect that:

- an offence has been or will be committed under any Act of Parliament; and
- tracking data that is in a person's possession or control will assist in investigation of the offence

A person subject to a section 487.017 production order with respect to tracking data previously preserved under a preservation demand (section 487.012) or a preservation order (section 487.013), shall destroy data that would not be retained in the ordinary course of business as soon as feasible after production is made under the section 487.017 order, or as soon as feasible after the order is revoked. The threshold of "reasonable grounds to suspect" is employed, and again, it already exists in current sections 487.013 and 492.1, and has been considered by the Supreme Court of Canada for other types of investigation.

Production Order for "financial data" (section 487.018)

This is a renumbered revision of the current section 487.013 order for a financial institution to produce information identifying an account holder. Like the existing provision, the amended version provides for production of names, addresses and dates of birth of account-holders, and the account type, account number, account status and dates on which the account was opened or closed. It does not provide for production of financial transaction data.

A judge would be empowered to make a production order if satisfied that there are reasonable grounds to suspect that:

- an offence has been or will be committed under any Act of Parliament; and
- data that is in the possession or control of a financial institution will assist in investigation of the offence.

Proposed section 487.018 is essentially the same as the existing section 487.013, enabling judges to order that financial institutions produce information identifying account-holders and accounts. Once such identifying information is obtained, an officer can apply to a judge for a general production order under section 487.014 to obtain records of financial transactions on the specified account(s).

Unfortunately, the section 487.018 heading, "Production order – financial data", raises the concern that financial transaction data may be produced without meeting the threshold for a general production order – which is reasonable grounds to *believe* that an offence "has been or will be committed" (proposed section 487.014.) The section 487.018 heading should be revised to confirm that the revised section has the same limited intent as the existing section 487.013.

RECOMMENDATION:

15. The CBA recommends that the heading "Production order – financial data" be revised to make clear that the new section 487.018 has the same limited intent as the existing section 487.013. The recommended revised heading is: "Production order for information identifying account-holders and accounts."

D. Tracking Warrants and Data Recorder Warrants

Warrant for Tracking Device (section 492.1)

This proposed section revises existing section 492.1, increasing the threshold for tracking individuals from "reasonable grounds to suspect" to "reasonable grounds to believe."

Under the revised provision, a judge could issue a warrant for a tracking device that pertains to "transactions or things" if satisfied that there are reasonable grounds to *suspect* that:

- an offence has been or will be committed under any Act of Parliament; and
- tracking the location of transactions or the location or movement of a thing, including a vehicle, will assist in investigation of the offence

A judge could issue a warrant for a tracking device that pertains to "a thing that is usually carried or worn by the individual" if satisfied that there are reasonable grounds to *believe* that:

- an offence has been or will be committed under any Act of Parliament; and
- tracking an individual's movement will assist in investigation of the offence

Warrant for Transmission Data Recorder (section 492.2)

This proposed section replaces the archaic section 492.1 warrant for telephone number recorders, with a new warrant for "transmission data recorders." Under the new provision, a judge could issue a warrant authorizing an officer to obtain "transmission data" by means of a transmission data recorder, if satisfied that there are reasonable grounds to *suspect* that:

- an offence has been or will be committed under any Act of Parliament; and
- transmission data will assist in investigation of the offence

Definition of "Transmission Data," and Implications

Materials accompanying Bill C-13 indicate that the purpose of the proposed transmission data provisions is to adapt current search and seizure provisions (coupled with judicial oversight) to the digital age, without significantly increasing police powers. The Bill's summary says:

> This enactment amends the *Criminal Code* to provide, most notably, for...
>
> > (d) a warrant that will extend the current investigative power for data associated with telephones to transmission data relating to all means of telecommunications

The CBA is concerned that this provision should not permit seizure of more information than permitted with pre-digital telephony. Digital transmission data is significantly different from pre-digital telephony signaling data. The Bill defines "transmission data" in the new sections 487.011 and 492.2(6):

> "transmission data" means data that
>
> (a) relates to the telecommunication functions of dialing, routing, addressing or signaling;
>
> (b) is transmitted to identify, activate or configure a device, including a computer program as defined in subsection 342.1(2), in order to establish or maintain access to a telecommunication service for the purpose of enabling a communication, or is generated during the creation, transmission or reception of a communication and identifies or purports to identify the type, direction, date, time, duration, size, origin, destination or termination of the communication; and
>
> (c) does not reveal the substance, meaning or purpose of the communication.

With pre-digital telephony, signaling data consisted of the number called from, the number called, whether the call was completed and the duration of the call. With digital communications, "transmission data" and what it reveals is different, including:

- the IP address of the originating computer
- the computer program being used
- the communications protocol being used (e.g. voice-over IP, video-conferencing)

- the IP address or domain name of the server or computer being communicated with
- whether the transmission was completed

While "content" is expressly excluded from the definition of transmission data, such data could provide some insight into the content of communications. The CBA is concerned that transmission data may provide law enforcement agencies with "biographical core" information, such as how frequently a person communicated with a particular health care provider. The privacy interest in such communications triggers the right to be free of unreasonable search and seizure under section 8 of the *Charter*.

RECOMMENDATION:

16. The Canadian Bar Association recommends that section 492.2(1) be amended to raise the threshold for a transmission data recorder warrant to "reasonable grounds to believe".

E. Conclusion

Most of the lawful access provisions of Bill C-13 would amend existing search and seizure provisions of the *Criminal Code* (with the exception of new provisions for preservation demands and preservation orders.) However, computer technology has resulted in a volume of data that could not have been imagined by the drafters of existing *Code* provisions and the same technology enables law enforcement agencies to seize unforeseen quantities of data by rapid electronic copying.

There is no *Criminal Code* provision for the return or destruction of copied personal information obtained lawfully by police agencies. Sections 489.1 and 490 of the *Code* provide a venerable and cumbersome regime for the return of "things" (exhibits) seized by police, but section 490(13) already permits police to retain, indefinitely, copies of seized documents. In Bill C-13, section 487.0192(4) extends that approach, providing that sections 489.1 and 490 do not apply to "documents" (derived from data) that are seized under any of the amended production order provisions (sections 487.014 to 487.018).

Although all seized data consists of "copies" from original encoding, the information content still comes into police possession. In addition to data seized under production orders, data

seized under tracking warrants and transmission data recorder warrants also could be characterized as "copies" subject to indefinite retention.

There are strong justifications for long-term retention of investigative information, but given the limited ambit of the *Criminal Code*, the *Code* amendments proposed in Bill C-13 do not sufficiently address privacy interests in the context of electronic investigation. The CBA urges that this issue be addressed outside of the mechanics of criminal procedure that are provided by the *Code* and by Bill C-13.

RECOMMENDATION:

17. The Canadian Bar Association recommends that the federal government conduct an independent comprehensive review of privacy interests in the context of electronic investigations, to go beyond the mechanical application of criminal procedure under the *Criminal Code* and Bill C-13.

IV. *COMPETITION ACT* AMENDMENTS

The CBA has concerns about the proposed amendments to the *Competition Act* in Bill C-13, and believes that those amendments should be subject to advance stakeholder consultations. Specifically, the Bill would:

- permit the Commissioner of Competition to use third party preservation and production orders available under the *Criminal Code* for investigations under the reviewable provisions of the *Competition Act*; and
- revise the definition of telemarketing in a manner that expands the scope of the Commissioner of Competition's investigative process

The most significant of these proposed changes is the application of criminal investigative tools to non-criminal matters. The CBA understands that Parliament's intention with Part VIII of the *Competition Act* is to distinguish between conduct which merits criminal sanction and conduct which, while subject to review by the Competition Tribunal, would otherwise be legal. Permitting criminal investigative powers to be used for enquiries under Part VIII of the Act erodes that distinction.

The *Competition Act* amendments proposed in Bill C-13 have significant implications for the administration and enforcement of the Act, and should be implemented only after further explanation and discussion of why such changes are required.

RECOMMENDATION:

18. **The Canadian Bar Association recommends that the *Competition Act* not be amended to permit use of third party preservation and production orders available under the *Criminal Code* for investigations under the non-criminal reviewable practices provisions of the legislation.**

19. **The Canadian Bar Association recommends that proposed changes to the *Competition Act* such as those in Bill C-13, with potential competition policy and enforcement implications, should be subject to advance stakeholder consultations.**

V. CONCLUSION

The CBA appreciates the opportunity to comment on Bill C-13, and to offer our suggestions to improve the Bill.