LIBRARY of PARLIAMENT
BIBLIOTHÈQUE du PARLEMENT

LEGISLATIVE SUMMARY

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

Publication No. 41-2-C13-E
11 December 2013

Julia Nicol
Dominique Valiquet

Legal and Social Affairs Division
Parliamentary Information and Research Service

Library of Parliament ***Legislative Summaries*** summarize government bills currently before Parliament and provide background about them in an objective and impartial manner. They are prepared by the Parliamentary Information and Research Service, which carries out research for and provides information and analysis to parliamentarians and Senate and House of Commons committees and parliamentary associations. Legislative Summaries are revised as needed to reflect amendments made to bills as they move through the legislative process.

Notice: For clarity of exposition, the legislative proposals set out in the bill described in this Legislative Summary are stated as if they had already been adopted or were in force. It is important to note, however, that bills may be amended during their consideration by the House of Commons and Senate, and have no force or effect unless and until they are passed by both houses of Parliament, receive Royal Assent, and come into force.

Any substantive changes in this Legislative Summary that have been made since the preceding issue are indicated in **bold print**.

Legislative Summary of Bill C-13
(Legislative Summary)

Publication No. 41-2-C13-E

Ce document est également publié en français.

CONTENTS

LEGISLATIVE SUMMARY OF BILL C-13: AN ACT TO AMEND THE CRIMINAL CODE, THE CANADA EVIDENCE ACT, THE COMPETITION ACT AND THE MUTUAL LEGAL ASSISTANCE IN CRIMINAL MATTERS ACT

1 BACKGROUND

On 20 November 2013, 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 (short title: Protecting Canadians from Online Crime Act) was introduced in the House of Commons by the Minister of Justice, the Honourable Peter MacKay.

1.1 PURPOSES OF THE BILL AND PRINCIPAL AMENDMENTS

Bill C-13 deals with:

- the offence of non-consensual distribution of intimate images;
- offences committed by means of telecommunication; and
- one aspect of the area of law generally referred to as “lawful access.”

Lawful access is an investigative technique used by law enforcement agencies and national security agencies that involves intercepting private communications and seizing information where authorized by law.

With regard to lawful access, Bill C-13 basically reintroduces the provisions of the former Bill C-30 – which was introduced in the 1st Session of the 41st Parliament and died on the *Order Paper* before second reading in the House of Commons – with the exception of its provisions concerning:

- the interception capability of telecommunications service providers; and
- warrantless requests for subscriber information.[1]

Bill C-13 creates two new criminal offences and aims to update Canadian criminal law. More specifically, the principal amendments in the bill:

- clarify that *Criminal Code* (Code) offences can generally be committed by any means of telecommunication, by ensuring therefore that offence provisions in the Code can apply expressly to cyberbullying and other criminal activities committed in cyberspace (clause 2);
- create a new criminal offence of non-consensual distribution of intimate images (clause 3);
- introduce judicial orders allowing for the prohibiting of the use of a computer or the Internet by an offender convicted of non-consensual distribution of intimate images (clause 3);

- introduce judicial orders authorizing the seizure and removal of intimate images (clauses 4 and 5);
- provide that if an authorization to intercept communications is given, a related warrant, such as a search warrant, may be issued at the same time (clauses 8, 9 and 11);
- extend the scope of the advocating genocide and hate propaganda offences to protect individuals on the basis of national origin, age, sex, or mental or physical disability (clause 12);
- create the offence of possession of a computer virus for the purpose of committing mischief (clause 17);
- make it possible for law enforcement agencies to make a demand or obtain a court order for the preservation of electronic evidence (clause 20);
- create new judicial production orders for obtaining data relating to the transmission of communications or data for tracking a thing or an individual (clause 20);
- create warrants for obtaining transmission data in real time and for the remote activation of tracking devices in certain types of technologies (clause 23);
- provide for the recovery of expenses incurred to obtain the removal of intimate images from the Internet (clause 24);
- introduce a recognizance order to be issued to prevent the distribution of intimate images (clause 25);
- ensure that the spouse of the person accused of non-consensual distribution of intimate images is considered a competent and compellable witness (clause 27);
- modernize the deceptive marketing practices offences in the *Competition Act* (clauses 33 to 35); and
- amend the *Mutual Legal Assistance in Criminal Matters Act* so that the new production orders can be used by Canadian authorities who receive assistance requests from other countries (clause 41).

1.2 Context

1.2.1 Cyberbullying

One aspect of the bill addresses cyberbullying, which has been in the news, particularly in relation to the high-profile cases of Rehtaeh Parsons and Amanda Todd. Rehtaeh Parsons attempted suicide in April 2013 (and was later taken off life support) after pictures of an alleged sexual assault were distributed which led to various types of bullying. Amanda Todd committed suicide in October 2012 after experiencing blackmail online and facing threats that topless pictures of her would be distributed on the Internet, a practice known as “sextortion.”

Also in October 2012, the federal, provincial and territorial ministers responsible for justice and public safety asked officials to look into potential gaps in the Code in relation to cyberbullying and the non-consensual distribution of intimate images. The resulting *Report to the Federal/Provincial/Territorial Ministers Responsible for Justice*

and Public Safety: Cyberbullying and the Non-consensual Distribution of Intimate Images was published in June 2013 and included recommendations that are integrated into Bill C-13.[2]

In December 2012, the Standing Senate Committee on Human Rights published a report on cyberbullying, *Cyberbullying Hurts: Respect for Rights in the Digital Age*. The report notes:

> Though there were differences of opinion regarding whether there is a need to update the [*Criminal*] *Code* for dealing with cyberbullying, a clear message endorsed by most witnesses was that when working with children, the restorative justice approach is most effective.[3]

1.2.2 International Obligations on Lawful Access

With regard to lawful access, Bill C-13 represents a step toward harmonizing the tools available to counter cybercrime in Canada with those of other countries, particularly regarding production orders and orders for the preservation of computer data.[4] Canada signed the Council of Europe's *Convention on Cybercrime* in November 2001, as well as its Additional Protocol on hate crime in July 2005.[5] The Convention requires states that are parties to the treaty to create offences under their domestic laws criminalizing certain uses of computer systems, and requires the adoption of legal tools adapted to deal with new technologies, such as orders to produce "subscriber information."

2 Description and Analysis

2.1 Amendments to the *Criminal Code*

2.1.1 Communication Includes Telecommunication (Clause 2)

Clause 2 amends section 4 of the Code by clarifying that where an offence has an element of communication, this includes communications made by any means of telecommunication, unless the means of communication are specified. This makes it clear that, as a general rule, the fact that an offence is committed using a telecommunications device does not bar a conviction for the offence.[6]

2.1.2 Distribution of Intimate Images

2.1.2.1 The New Offence (Clause 3)

Clause 3 creates a new offence of *knowingly* publishing, distributing, transmitting, selling, making available or advertising an "intimate image" of a person. Under this provision, contained in new section 162.1 of the Code, making, possessing or accessing such an image does not appear to be grounds for a charge, which is unlike the child pornography offences outlined in section 163.1 of the Code.

An “intimate image” for the purposes of the new provision is defined as a visual recording (as opposed to written materials or audio recordings, for example) by means of a photographic, film or video recording. It must be of a person:

- in the nude; or
- exposing his or her genital organs or anal region or breasts; or
- engaged in explicit sexual activity.

In addition, a conviction requires that, *at the time of the recording*, there must have been circumstances that gave the depicted person a reasonable expectation of privacy. This reasonable expectation of privacy must also exist *at the time the offence is committed* (for example, when the picture is distributed to others). What constitutes a reasonable expectation of privacy in the context of the new provision will be determined by the courts.[7]

As well, the person in the image must not have consented to its distribution or the accused must have been reckless[8] as to whether that person consented.

Finally, where the conduct in question serves the public good and does not extend beyond what serves the public good, a person cannot be convicted of the new offence.[9]

This is a hybrid offence, that is, the prosecutor will have the option of proceeding by indictment or summary conviction. The offence is punishable on indictment by up to five years’ imprisonment or, upon summary conviction, to a fine of not more than $5,000 and/or six months’ imprisonment.[10]

2.1.2.1.1 Comparison with the Child Pornography and Voyeurism Offences

Most of the recommendations contained in the June 2013 *Report to the Federal/Provincial/Territorial Ministers Responsible for Justice and Public Safety: Cyberbullying and the Non-consensual Distribution of Intimate Images* prepared by the Coordinating Committee of Senior Officials Cybercrime Working Group are integrated into Bill C-13. The report notes that some members of the working group found that child pornography charges are “too blunt an instrument” to address the non-consensual distribution of intimate images, particularly where the accused is under 18. They distinguished between cases where the issue is more one of a breach of privacy than of sexual exploitation of children, and some working group members expressed concern that child pornography charges might be inappropriate in some cases. It was felt that if such charges were applied, an unwanted expansion of the exceptions to the child pornography provisions might develop.[11] The new offence addresses these concerns.

However, new section 162.1 concerning “intimate images” may lead to an unintended result. Under this provision, the perpetrator cannot be convicted if the person in the image consented to the distribution of the image, whereas under the provision of the Code regarding child pornography (section 163.1), consent cannot

be used as a defence. This difference may have the following consequence in cases where the images disseminated depict an individual under the age of 18:

- If the individual *did consent* to the distribution, the perpetrator would likely be charged not under new section 162.1, which allows consent as a defence, but under section 163.1, which does not.
- If the individual *did not consent* to the distribution, the perpetrator could be charged under either section, since the defence of consent would not apply.

Since the penalty for child pornography is greater and includes a mandatory minimum sentence,[12] an accused could end up with a harsher sentence in cases where consent was given than in those where it was not.

It appears as well that the new provision does not provide a limitation on the age at which a minor could consent to the distribution of such an image. Bill C-13 does not add the new offence to section 150.1 of the Code, which outlines the sexual offences for which consent is not a defence, as well as the rules relating to age of consent.

Nudity of a non-sexual nature appears to be sufficient to meet the requirements of the new offence.[13] In contrast, nudity is not sufficient for a conviction for child pornography. That offence includes terms such as “for a sexual purpose” and “the dominant characteristic of which is … a sexual organ.” Even with these restrictions, the Supreme Court of Canada felt it necessary to clarify in *R. v. Sharpe* that nude baby pictures and non-sexual nudity were not covered by the child pornography offence.[14]

Finally, the child pornography provisions of the Code use the terms “sexual organ or the anal region,” whereas the new offence of distributing an intimate image, along with existing provisions in sections 162 and 171.1, use the terms “genital organs,” “anal region” and “breasts.” It is not clear whether the terms imply something different. They seem likely to cover the same areas of the body, but the use of different words may be seen as implying different meanings.[15]

Below is a table comparing the proposed new offence with the existing offences of voyeurism and child pornography.

Table 1 – Comparison of New *Criminal Code* Section 162.1 (Distribution of Intimate Images) and Existing Provisions

Elements of the Offence	New Section 162.1 (Distribution of Intimate Images)	Section 162 (Voyeurism)	Section 163.1 (Child Pornography)
Recording format	Visual recording by photographic, film, video or other recording	Visual recording by photographic, film, video or other recording made by any means[a]	Photographic, film, video or other visual representation, whether or not made by electronic or mechanical means[b]
Content of images	Full nudity, genital organs, anal region, breasts or engaged in explicit sexual activity	Full nudity, genital organs, anal region, breasts or engaged in explicit sexual activity[c]	Sexual organ or anal region where they are depicted for a sexual purpose or explicit sexual activity
Reasonable expectation of privacy required for conviction?	Yes	Yes	No
Types of acts criminalized	Knowingly publishing, distributing, transmitting, selling, making available or advertising	Recording, printing, copying, publishing, distributing, circulating, selling, advertising or making public or possession for any of those purposes	163.1(2): Making, printing, publishing or possessing for the purpose of publication 163.1(3): Transmitting, making available, distributing, selling, advertising, importing, exporting or possessing for the purpose of transmission, making available, distributing, sale, advertising or exporting 163.1(4): Possessing 163.1(4.1): Accessing
Consent	Lack of consent or recklessness as to whether there was consent is required to prove the offence	The recording must be surreptitious	A person cannot consent to child pornography
Age of person in the recording	No age limitations	No age limitations	Under the age of 18 (or depicted as being under the age of 18 where engaged in sexual activity)

Elements of the Offence	New Section 162.1 (Distribution of Intimate Images)	Section 162 (Voyeurism)	Section 163.1 (Child Pornography)
Maximum punishment	Five years on indictment; $5,000 and/or six months on summary conviction	Five years on indictment; $5,000 and/or six months on summary conviction	163.1(2) and (3): Ten years on indictment, with a one-year mandatory minimum sentence; two years less a day on summary conviction, with a six-month mandatory minimum sentence 163.1(4) and (4.1): Five years on indictment, with a mandatory minimum sentence of six months; 18 months on summary conviction, with a mandatory minimum sentence of 90 days
DNA data bank order	Under certain conditions	Under certain conditions	Mandatory[d]
Registry on the Sex Offender Registry	No	Under certain conditions[e]	Mandatory[f]
Exclusions/Defences	If the conduct that forms the subject-matter of the charge serves the public good and does not extend beyond what serves the public good	If the conduct that forms the subject-matter of the charge serves the public good and does not extend beyond what serves the public good	Legitimate purposes relating to the administration of justice or to science, medicine, education or art where there is no undue risk of harm to persons under the age of 18 According to *R. v. Sharpe*: Private recordings of lawful sexual activity held for private use

a. Section 162 of the Code includes not only recording, but also observations by mechanical or electronic means; however, this is not relevant to the comparison with new section 162.1.

b. Section 163.1 of the Code also includes provisions relating to using a visual representation to advocate or counsel sexual activity with a person under the age of 18, written materials and audio recordings, but this is not relevant to the comparison with new section 162.1.

c. The offence is committed even where there is no nudity or sexual activity, but where the recording is done for a sexual purpose; see section 162(1)(*c*) of the Code.

d. See Code, ss. 487.04 and 487.051(1).

e. Ibid., ss. 490.011(1)(*b*) and 490.012(2).

f. Ibid., ss. 490.011(1)(*a*) and 490.012(1).

2.1.3 Warrants Related to Intimate Images (Clauses 4, 5 and 7)

A judge may currently issue a warrant to authorize seizure of copies of a voyeuristic recording, obscene publications, crime comics[16] and child pornography under section 164 of the Code. The judge can also order the forfeiture of such materials for disposal or the restoration of the items if they are not found to meet the definition of the relevant provision. Clause 4 of Bill C-13 adds intimate images to that list, allowing judges to authorize the seizure and forfeiture of such images. (More information on forfeiture is found in section 2.1.4.2 of this Legislative Summary.)

In addition, section 164.1 currently allows the court to order the custodian of a computer system on which there are voyeuristic images, child pornography or associated data to:

- provide the court with a copy;
- ensure that the material is not stored and available through the computer system; and
- provide information to identify and locate the person who posted the material.

This section was created to allow for the shutting down of child pornography and voyeuristic websites. Clause 5 adds intimate images to the list of materials for which a court order may be obtained under section 164.1.

Finally, clause 7 of the bill adds the offence of non-consensual distribution of intimate images to the list in section 183 of the Code of the offences for which judicial authorization for electronic interception of a private communication can be obtained. This means that law enforcement agencies will be able to use electronic surveillance to investigate this new offence.

2.1.4 Related Orders (Clauses 3, 6, 24 and 25)

Bill C-13 allows the court to grant a number of orders to address various concerns relating to the distribution of intimate images.

2.1.4.1 Restriction on Internet Use (Clause 3)

Clause 3 also provides that, where an offender is convicted or given a conditional discharge for the offence outlined in new section 162.1, the court that sentences or discharges the offender may also make an order prohibiting the offender from using the Internet or other digital network except in accordance with any conditions that may be set by the court. The order may be for any period that the court considers appropriate, including during imprisonment. Non-compliance with such an order is a hybrid offence that may result in up to two years' imprisonment upon conviction.

2.1.4.2 Forfeiture (Clause 6)

Section 164.2 currently allows that, upon conviction for a number of specified offences and the application of the Attorney General, anything other than real property (real estate, etc.) that was used in the offence and is the property of a party to the offence, or was transferred for the purpose of avoiding forfeiture, may be forfeited. Clause 6 of Bill C-13 adds new section 162.1 to the list of offences to which section 164.2 applies.

2.1.4.3 Restitution Order (Clause 24)

Section 738 of the Code allows for restitution orders to be made in certain circumstances, such as when an offender has damaged property or caused the victim to incur costs like those to re-establish her or his identity or credit history.

Clause 24 allows for a restitution order to be made where there is a conviction under new section 162.1 and a person has incurred costs to have the intimate image removed from the Internet or other digital network.

2.1.4.4 Peace Bond (Clause 25)

Clause 25 adds a new justification for the granting of a surety to keep the peace (a peace bond) under section 810 of the Code where a person fears on reasonable grounds that another person will commit an offence under new section 162.1.

2.1.5 Testimony of a Spouse (Clause 27)

There is a general common law rule that the spouse of an accused is not competent or compellable to testify for the Crown, with a number of exceptions,[17] some of which are outlined in section 4 of the *Canada Evidence Act*.[18] Bill C-13 amends the *Canada Evidence Act* to provide a new exception to make the wife or husband of a person charged under new section 162.1(1) a compellable witness, meaning that he or she could be required by the prosecution to testify against the accused.

2.1.6 Interception of Private Communications: Related Warrants (Clauses 8 to 11)

Part VI of the Code ("Invasion of Privacy," section 183 and following) is the centrepiece of federal legislation on electronic surveillance by law enforcement agencies ("wiretapping") and applies to all offences enumerated in section 183 of the Code. Addressing the interception of the contents of oral communications or video footage and often involving a serious invasion of privacy, Part VI sets out stricter conditions for the issuance of a judicial authorization to intercept private communications than for the granting of a search warrant or a production order.[19]

While the Code provisions regarding search and seizure were amended in the 1980s and 1990s to expressly include computers, most provisions in Part VI date back to 1974.

Police forces often use electronic surveillance in conjunction with other investigative techniques. Given that an application for judicial authorization to intercept communications is sometimes based on the same information as that presented in support of an application for a warrant – a search warrant, for example – or may come from the same source, the bill allows the judge to give an authorization to intercept communications and, at the same time, issue the requested warrant.

Regardless of whether the interception is done with the consent of one of the parties to the communication (section 184.2 of the Code), without the consent of the parties (sections 185 and 186 of the Code) or for a maximum period of 36 hours in an emergency (section 188 of the Code), under Bill C-13 the judge can, in addition to giving an authorization to intercept, issue a search warrant, a general warrant, make a general production order, make a specific production order to obtain certain information (such as computer data or financial information), make an assistance order or issue a warrant to use a tracking device or a "transmission data recorder"

(clauses 8, 9 and 11). These clauses are intended to allow police officers to more quickly investigate past or possible future offences.

All documents relating to an application for authorization to intercept communications are confidential; that is why they are placed in a packet sealed by the judge (section 187 of the Code). Clause 10 of the bill provides that all documents relating to a request for a related warrant or order in connection with an authorization can be sealed at the same time.

2.1.7 Genocide and Hate Propaganda (Clause 12)

Section 318 of the Code criminalizes advocating genocide against certain "identifiable groups," which are listed. Currently, the identifiable groups are defined as including those distinguished by colour, race, religion, ethnic origin or sexual orientation. Clause 12 adds national origin, age, sex and mental or physical disability to the definition. Since section 319, which criminalizes incitement of hatred (commonly known as the hate speech provision), relies on the definition of "identifiable group" in section 318, Bill C-13 also criminalizes hate speech on the basis of national origin,[20] age, sex and mental or physical disability.[21]

2.1.8 Device for Theft of Telecommunication Services (Clause 15)

At present, section 327 of the Code makes it a crime to possess, manufacture or sell a device used for the theft of telecommunication services. Clause 15 of the bill essentially adds the offences of importing such a device or making it available. As well, the bill makes this indictable offence a hybrid offence, giving the prosecutor the choice of proceeding by indictment or by summary conviction.

2.1.9 Computer Virus (Clause 17)

Under the existing provisions of the Code, only spreading or attempting to spread a computer virus[22] constitutes an offence.[23] In accordance with the requirements of the *Convention on Cybercrime*,[24] clause 17 of the bill makes it illegal to possess a computer virus for the purpose of committing mischief, and also makes it an offence to import and make available a computer virus.

2.1.10 False, Indecent or Harassing Communications (Clause 18)

The existing provisions of the Code regarding the offences of sending a message in a false name and sending false information, indecent remarks or "harassing" messages (the French term *harassants* currently used in section 372(3) of the Code is replaced by *harcelants* in the bill) refer to certain communication technologies used to commit those offences, such as telegram, radio and telephone.[25] Clause 18 of the bill amends those offences by removing the references to those specific communications technologies and, for some of those offences, substituting a reference to any means of telecommunication. As a result, it will be possible, for instance, to lay charges for offences related to cyberbullying, regardless of the transmission method or technology used.

Additionally, the bill provides that the offences consisting of transmitting false information, indecent remarks or harassing messages, currently punishable by summary conviction, will now be hybrid offences. Accordingly, the maximum sentence for the offences relating to indecent and harassing communications will be increased to imprisonment for two years, in the event that the prosecutor decides to proceed by indictment.

2.1.11 Preservation Demand and Order (Clause 20)

Information in electronic form may be easily and quickly destroyed or altered. Clause 20 of the bill therefore adds a new investigative tool to the Code to preserve this type of evidence. This tool may take one of two forms: a preservation demand or a preservation order. A preservation demand is made by a peace officer (new section 487.012 of the Code), while a preservation order is made by a judge, on application by a peace officer (new section 487.013 of the Code).

A preservation demand or order directs a person, such as an Internet service provider (ISP), to preserve "computer data"[26] that are "in their possession or control" when they receive the demand or order. A telecommunications service provider may also *voluntarily* preserve data and provide it to a law enforcement agency, even where there is no preservation demand or order, without incurring any criminal or civil liability (new section 487.0195 of the Code).[27]

This new investigative tool is different from the data retention measure in effect in some countries,[28] which compels telecommunications service providers to collect and retain data for a prescribed period for all their subscribers, whether or not they are the subjects of an investigation. In contrast, a preservation demand or order relates only to a particular telecommunication or person, in the context of a police investigation.

A preservation demand or order may be given to a telecommunications service provider only where there are "reasonable grounds to suspect" that an offence has been or will be committed (new sections 487.012(2) and 487.013(2) of the Code). However, a preservation demand or order may not be made to the person suspected of having committed an offence (new sections 487.012(3) and 487.013(5) of the Code). It is of note that the test of *reasonable grounds to suspect* that an offence has been or will be committed is less stringent than the usual requirement, *reasonable grounds to believe* that an offence has been or will be committed. Although the *reasonable grounds to suspect* requirement is rarer, it is currently provided in certain other provisions of the *Criminal Code*.[29]

Preservation demands and orders are temporary measures: they are generally in effect long enough to allow the law enforcement agency to obtain a search warrant or production order. The maximum length of a preservation demand is 21 days in the case of an offence committed under federal law or 90 days in the case of an offence committed under a law of a foreign state, and the demand may be made only once (new sections 487.012(4) and 487.012(6) of the Code); the maximum length of a preservation order is 90 days and may be renewed (new sections 487.013(6) and 487.194(2) of the Code).

A person who receives a preservation demand or order is required, after the demand or order expires, or after the data have been given to the law enforcement agency under a production order or search warrant, to destroy the computer data that would not be retained in the ordinary course of business (new sections 487.0194 and 487.0199 of the Code).

Contravention of a preservation demand is an offence punishable by a maximum fine of $5,000 (new section 487.0197 of the Code). Contravention of a preservation order is an offence punishable by a maximum fine of $250,000 or imprisonment for a maximum term of six months, or both (new section 487.0198 of the Code).

2.1.12 Production Orders (Clause 20)

A production order is made by a judge and is similar to a search warrant. The difference lies in the way in which the information is obtained: under a production order, the person in possession of the information must produce it on request, whereas under a search warrant, the law enforcement agency goes to the site to obtain the information by searching for it and seizing it. A law enforcement agency with a production order is able to more readily obtain documents that are in another country, for example.

The Code already provides a procedure for obtaining a *general* production order, that is, an order that applies regardless of the type of information a law enforcement agency is seeking.[30] Issuance of the order is based on the existence of *reasonable grounds to believe* that an offence has been committed. The Code also provides for *specific* production orders, that is, orders for obtaining certain precise information, such as banking information or telephone call logs.[31] Issuance of specific production orders is based on the less stringent *reasonable grounds to suspect* that an offence has been or will be committed.

Clause 20 of the bill creates new types of specific production orders, issuance of which is based on the existence of reasonable grounds to suspect that an offence has been or will be committed. They allow a peace officer to obtain two types of information from a telecommunications service provider:[32] “transmission data” (new section 487.016 of the Code) and “tracking data” (new section 487.017 of the Code).[33]

Essentially, “transmission data” are data that indicate the origin, destination, date, time, duration, type and volume of a telecommunication (e.g., a telephone call or an Internet communication), but do not include the content of the telecommunication.[34] This type of data is useful: for example, it may be used to trace all telecommunications service providers involved in the transmission of data in order to identify the initial telecommunications service provider and thus determine the origin of a telecommunication (new section 487.015 of the Code). “Tracking data” relate to the location of a thing or individual.

These new types of production orders allow law enforcement agencies to obtain *historical* transmission or tracking data, that is, data already in the possession of the telecommunications service provider when it receives the order. To obtain these types of data *in real time*, law enforcement agencies need a warrant.

A review procedure is provided for challenging any type of production order, existing or new (new section 487.0193 of the Code).[35] A person who has received an order may apply to a judge to revoke or vary it if production is unreasonable[36] or discloses privileged information.[37] As in the case of a preservation order, violation of a production order is punishable by a maximum fine of $250,000 or imprisonment for a maximum term of six months, or both (new section 487.0198 of the Code).

2.1.13 Warrant for a Tracking Device (Clause 23)

At present, section 492.1 of the Code allows a peace officer with a warrant[38] to secretly install a tracking device (e.g., a GPS device) on a thing, if there are reasonable grounds to suspect that an offence has been or will be committed and if it appears that the use of such a tracking device could provide information that would assist in the police investigation, notably the whereabouts of a person.

Clause 23 of the bill retains this type of warrant, but makes a distinction between a warrant to install a tracking device on a *thing*, such as a vehicle, to track its movements (new section 492.1(1) of the Code), and a warrant to install that kind of device on a thing *usually carried or worn by an individual*, such as a cellphone, in order to track the individual's location and movements (new section 492.1(2) of the Code). A warrant to track the movements of a thing is based on the existing standard of *reasonable grounds to suspect* that an offence has been or will be committed, while a more stringent standard applies to a warrant to track the movements of an individual: the existence of *reasonable grounds to believe* that an offence has been or will be committed.

In addition to allowing a tracking device to be *installed*, the bill allows law enforcement agencies to *remotely activate* devices of the kind that are found in certain types of technology, such as cellphones or the GPS devices in certain cars (new section 492.1(3) of the Code).

The maximum duration of a warrant for a tracking device is still 60 days. However, that period is extended to one year in the case of a terrorism or organized crime offence (new sections 492.1(5) and 492.1(6) of the Code).[39]

2.1.14 Warrant for a Transmission Data Recorder (Clause 23)

At present, section 492.2(1) of the Code allows a peace officer with a warrant to secretly install a number recorder on a telephone or telephone line, if there are reasonable grounds to suspect that an offence has been or will be committed and if it appears that the use of this kind of recorder could provide information that would assist in the police investigation. The law enforcement agency could thus obtain the "incoming" and "outgoing" telephone numbers for a telephone that was being tapped.

Clause 23 of the bill provides for a warrant that authorizes a peace officer to install and activate a transmission data recorder[40] (new section 492.2 of the Code). As before, the warrant will allow law enforcement agencies to obtain telephonic data, but also to obtain data indicating the origin and destination of an Internet communication, for example. Police services will thus be able to have access to this transmission data in real time. As in the case of a warrant to install a telephone number recorder, the new type of warrant is based on the requirement that there are reasonable grounds to suspect that an offence has been or will be committed. Lastly, Bill C-13 does not provide for the use of a transmission data recorder without a warrant in emergencies, contrary to the provisions set out in former Bill C-30.

2.2 Amendments to the *Competition Act*

2.2.1 Preservation and Production Orders (Clause 29)

The new provisions of the Code concerning demands and orders for the preservation of computer data and orders for the production of transmission data and banking information will apply to certain investigations under the *Competition Act*. The Commissioner of Competition will thus be able to use these new investigative tools to obtain evidence relating to deceptive marketing practices and restrictive trade practices.

2.2.2 Modernization of Offences (Clauses 33 to 35)

Clauses 33 to 35 of the bill modernize certain offences related to deceptive marketing practices offences, such as deceptive telemarketing and making misrepresentations about a product or service, and replace the reference to "telephone" as the means of committing these offences with "any means of telecommunication" used for communicating orally.

2.3 Amendments to the *Mutual Legal Assistance in Criminal Matters Act*

The *Mutual Legal Assistance in Criminal Matters Act* was enacted in 1988 and gives Canadian courts the power to issue compulsory measures, such as subpoenas and search warrants, to obtain evidence in Canada on behalf of a foreign state for use in a criminal investigation and prosecution being conducted by that state. The legislation aims to promote cooperation among certain states by establishing a system for exchanging information and evidence.[41]

2.3.1 Searches by the Commissioner of Competition (Clause 37)

The bill authorizes the Commissioner of Competition to execute search warrants issued under the *Mutual Legal Assistance in Criminal Matters Act*.

2.3.2 Production Orders (Clause 41)

The bill provides that the production orders for obtaining banking information, transmission data or tracking data described in the Code may be used by Canadian authorities who receive assistance requests from their international partners.

2.4 Coming into Force (Clause 47)

Clause 47 provides that the provisions of Bill C-13, except the coordinating amendments, will come into force three months after the day on which the bill receives Royal Assent.

NOTES

1. For more information on these topics, see Erin Shaw and Dominique Valiquet, *Legislative Summary of Bill C-30: An Act to enact the Investigating and Preventing Criminal Electronic Communications Act and to amend the Criminal Code and other Acts*, Publication no. 41-1-C30-E, Parliamentary Information and Research Service, Library of Parliament, Ottawa, 15 February 2012, ss. 2.1.1 and 2.1.2.
2. CCSO [Coordinating Committee of Senior Officials] 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.
3. Senate, Standing Committee on Human Rights, *Cyberbullying Hurts: Respect for Rights in the Digital Age*, December 2012.
4. For more information on international lawful access legislation, see Christopher Parsons, *Lawful Access and Data Preservation/Retention: Present Practices, Ongoing Harm, and Future Canadian Policies*, 7 February 2012.
5. Council of Europe, *Convention on Cybercrime*, 23 November 2001, ETS [European Treaty Series] No. 185, art. 18 (in force 1 July 2004); Council of Europe, *Additional Protocol to the Convention on Cybercrime, concerning the criminalisation of acts of a racist and xenophobic nature committed through computer systems*, 28 January 2003, ETS No. 189 (in force 1 March 2006).
6. Hedy Fry, MP, has proposed a number of bills that would have made the same clarification with respect to certain offences, the most recent being Bill C-273 in the 1st Session of the 41st Parliament.
7. The same term is found in section 162 (voyeurism) of the *Criminal Code* (Code), which may be of some assistance in interpretation, though that is a relatively new provision as well. It was introduced in 2005, and thus far there is only limited jurisprudence related to it. Being naked or involved in sexual activities in a bedroom, for example, have been found to be circumstances giving rise to a reasonable expectation of privacy: see *Regina v. Coombs*, 2013 ONSC 5243 (CanLII); *R. v. Larouche*, 2012 CM 3009 (CanLII); and *R. v. Keough*, 2011 ABQB 48 (CanLII) (sentence varied on appeal). A reasonable expectation of privacy was also found in a case where a man videotaped young girls at a park from his van: see *R. v. Rudiger*, 2011 BCSC 1397 (CanLII). It does not appear that any Court of Appeal has defined the scope of the reasonable expectation of privacy in the context of section 162.

8. The Supreme Court of Canada, in *Sansregret v. The Queen*, defined recklessness as the conduct of, "one who, aware that there is danger that his conduct could bring about the result prohibited by the criminal law, nevertheless persists, despite the risk. It is, in other words, the conduct of one who sees the risk and who takes the chance" (para. 16). However, in *Sansregret*, the Court did not set out the degree of risk required to attract criminal sanction. With regard to the offence of counselling an offence that is not committed (s. 464 of the Code), the Court set out this degree as being "substantial and unjustified" (*R. v. Hamilton*, [2005] 2 S.C.R. 432, para. 29).

9. The same is true for sections 162 (voyeurism) and 163 (corrupting morals) of the Code. In the 2001 case of *R. v. Sharpe*, [2001] 1 SCC 45, the Supreme Court of Canada discussed the public good defence in the context of a child pornography charge, an offence for which there was a public good defence at the time. Though not providing a comprehensive analysis, the Court provided some examples of a public good that could be applicable in the context of the distribution of intimate images, including for the purpose of prosecution, for work on the political or philosophical aspects of the topic or "promot[ing] expressive or psychological well-being or enhanc[ing] one's sexual identity in ways that do not involve harm to others" (para. 71).

10. Note that the punishment for summary conviction is contained in section 787 of the Code, not in new section 162.1.

11. *R. v. Sharpe* created a "personal use" exception to section 163.1 to allow recording where two youths are engaged in legal sexual activity as long as it is for their own personal use.

12. The offence of child pornography is a hybrid offence and, on indictment, carries a five- or ten-year maximum, and a six-month or one-year mandatory minimum sentence, depending on the subsection under which the charge is laid. The new offence – also a hybrid offence – on indictment carries a five-year maximum but no minimum mandatory sentence.

13. This could potentially include emailing a photo of a naked baby to grandparents or of a diaper rash to the doctor, for example, though the courts may interpret such scenarios as fitting within the public good exception.

14. *R. v. Sharpe*, para. 73.

15. *Roget's International Thesaurus* (5th ed., Robert L. Chapman, HarperCollins Publishers, 1992), for example, treats "sex organ" as a synonym for "genitals" but states that breasts are a secondary sex characteristic, so it is not clear if breasts would be included.

16. The definition of a crime comic is found in section 163(7) of the Code.

17. See *R. v. Hawkins*, [1996] 3 S.C.R. 1043, for more on this topic.

18. Case law is divided on the question of whether section 4 of the *Canada Evidence Act* applies to persons in a common-law relationship. For instance, the Ontario Superior Court of Justice has stated: "[T]he common-law rule of spousal incompetency which is limited to unions recognized by provincial law involving wives and husbands offends s. 15(1) of the *Charter of Rights and Freedoms* " (*R. v. Edenlenbos*, (2000) 7 C.R.R. (2d) 154). However, in 2009, the Saskatchewan Court of Appeal was of the opposite opinion when it found that neither the common law spousal incompetency rule nor section 4 applies to persons in a common-law relationship (*R. v. Martin* (2009), 64 C.R. (6th) 377).

19. For more information on production orders, see section 2.1.12 of this Legislative Summary.

20. The definition in article 2 of the *Additional Protocol to the Convention on Cybercrime, concerning the criminalisation of acts of a racist and xenophobic nature committed through computer systems* also includes national origin. Article 20 of the protocol's "Explanatory Report" reads as follows:

> The notion of "national origin" is to be understood in a broad factual sense. It may refer to individuals' histories, not only with regard to the nationality or origin of their ancestors but also to their own national belonging, irrespective of whether from a legal point of view they still possess it. When persons possess more than one nationality or are stateless, the broad interpretation of this notion intends to protect them if they are discriminated on any of these grounds. Moreover, the notion of "national origin" may not only refer to the belonging to one of the countries that is internationally recognised as such, but also to minorities or other groups of persons, with similar characteristics.

21. Note that there is a separate regime to address hate speech under the *Canadian Human Rights Act*, though a private member's bill, Bill C-304, resulted in the repeal of those provisions in June 2013. The repeal will come into force one year from that time.

22. In this Legislative Summary, the term "computer virus" includes other malicious code, such as computer worms.

23. Code, s. 430(1.1). See also s. 342.2.

24. *Convention on Cybercrime*, art. 6.

25. Code, ss. 371 and 372.

26. The definition of "computer data" is given in clause 20(4) of the bill. Essentially, it means data that can be processed by computer.

27. The federal Minister of Justice, Peter Mackay, has specified that this immunity only applies if the voluntary disclosure is in accordance with the provisions of the law, such as the *Personal Information Protection and Electronic Documents Act* (see s. 7(3) of this Act): see House of Commons, Standing Committee on Justice and Human Rights, *Evidence*, 28 November 2013.

28. See European Parliament, *Directive 2006/24/EC of the European Parliament and of the Council of 15 March 2006 on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC*, L 105/54.

29. For examples of the use of reasonable grounds to suspect, see Code, ss. 83.3 (terrorism), 254 (impaired driving), 487.13 (production order for financial information), 492.1 (tracking warrant), 492.2 (number recorder warrant) and 529.3 (enter dwelling without warrant in emergency). For a judicial definition of reasonable grounds to suspect, see *R. v. Cahil* (1992), 13 C.R. (4th) 327 (B.C. C.A.). See also the "Statement from the Privacy Commissioner of Canada regarding Bill C-13," Ottawa, 28 November 2013.

30. Code, s. 487.012. See also new section 487.014, added by the bill, which provides for a similar general production order.

31. Code, ss. 487.013(1), 487.013(4) (see also new section 487.018, added by the bill) and 492.2(2).

32. The peace officer may also obtain this information from another person – but not from the suspect in a police investigation – who has the data in his or her possession or control.

33. See the definitions of these types of data in new section 487.011 of the Code, added by the bill.

34. Article 1 of the *Convention on Cybercrime* contains a similar definition, but uses the term "traffic data."

35. A similar procedure is currently provided in section 487.015 of the Code.

36. A Supreme Court of Canada ruling shed light on the matter of compensating a telecommunications service provider for costs associated with executing a production order for call data (section 487.012 of the *Criminal Code)*. The Court ruled that various factors should be taken into account, including the breadth of the order being sought, the size and economic viability of the object of the order, and the extent of the order's financial impact on the telecommunications service provider: see *Tele-Mobile Co. v. Ontario*, [2008] 1 S.C.R. 305.

37. A production order may contain conditions to protect information covered by solicitor–client privilege: see new section 487.019(1) of the Code, added by the bill.

38. Where there are exigent circumstances and the conditions for obtaining a warrant exist, a warrant is not necessary. The same is true for a search and a transmission date recorder: see Code, s. 487.11; see also clause 26 of the bill.

39. This lengthened duration of the warrant is consistent with the current situation relating to wiretapping for terrorism and organized crime offences: see Code, s. 186.1.

40. See the definition in new section 492.2(6) of the Code.

41. Public Prosecution Service of Canada, "Mutual Legal Assistance in Criminal Matters," Chapter 43 in Part VIII, "International Assistance," in *The Federal Prosecution Service Deskbook*.