S.C.C. File No. 36435

IN THE SUPREME COURT OF CANADA
(ON APPEAL FROM THE COURT OF APPEAL FOR ALBERTA)

BETWEEN:

HER MAJESTY THE QUEEN

APPELLANT
(Respondent)

AND:

OSWALD OLIVER VILLAROMAN

RESPONDENT
(Appellant)

AND:

ATTORNEY GENERAL OF BRITISH COLUMBIA,
CRIMINAL LAWYERS' ASSOCIATION OF ONTARIO

INTERVENERS

FACTUM OF THE INTERVENER ATTORNEY GENERAL OF BRITISH COLUMBIA
Rule 42, *Rules of the Supreme Court of Canada*

DANIEL M. SCANLAN
Ministry of Justice and Attorney General
3rd Floor, 940 Blanshard Street
Victoria, British Columbia V8W 3E6
Tel: (250) 387-0284
Fax: (250) 387-4262
E-Mail: daniel.scanlan@gov.bc.ca

Counsel for the Intervener, Attorney General of British Columbia

ROBERT E. HOUSTON, Q.C.
Burke-Robertson, Barristers & Solicitors
Suite 200 - 441 MacLaren Street
Ottawa, Ontario K2P 2H3
Tel: (613) 236-9665
Fax: (613) 235-4430
E-Mail: rhouston@burkerobertson.com

Ottawa Agent for the Intervener, Attorney General of British Columbia

JOLAIN ANTONIO
JASON WUTTUNEE
Alberta Justice, Criminal Division
3rd floor, Centrium Place, 6 Ave. S.W.
Calgary, Alberta T2P 0B2
Tel: (403) 297-6005
Fax: (403) 297-3453
E-Mail: jolaine.antonio@gov.ab.ca

Counsel for the Appellant, Her Majesty the Queen

D. LYNNE WATT

Gowling Lafleur Henderson LLP
160 Elgin Street
Ottawa, Ontario K1P 1C3
Tel: (613) 786-8695
Fax: (613) 788-3509
E-Mail: lynne.watt@gowlings.com

Ottawa Agent for the Appellant, Her Majesty the Queen

IAN D. MCKAY
HEATHER FERG
Evans Fagan Rice McKay
203, 1117 1st Street S.W.
Calgary, Alberta T2R 0T9
Tel: (403) 517-1777
Fax: (403) 517-1776
Email : ian@mckaycriminaldefence.com

Counsel for the Respondent, Oswald Oliver Villaroman

MARIE-FRANCE MAJOR
Supreme Advocacy LLP
100- 340 Gilmour Street
Ottawa, Ontario
K2P 0R3
Tel: (613) 695-8855 Ext: 102
Fax: (613) 695-8580
E-mail: mfmajor@supremeadvocacy.ca

Ottawa Agent for the Respondent, Oswald Oliver Villaroman

SHARON E. LAVINE
NAOMI M. LUTES
Greenspan Humphrey Lavine
2714 – 130 Adelaide Street West
Toronto, Ontario M5H 3P5
Tel: (416) 868-1755
Fax: (416) 868-1990

Counsel for the Intervener, Criminal Lawyers' Association of Ontario

NADIA EFFENDI
Borden Ladner Gervais LLP
World Exchange Plaza
Suite 1300, 100 Queen Street
Ottawa, Ontario K1P 1J9
Tel: (613) 237-5160
Fax: (613) 230-8845
Email: neffendi@blg.com

Ottawa Agent for the Intervener, Criminal Lawyers' Association of Ontario

TABLE OF CONTENTS

Page

PART I – OVERVIEW AND STATEMENT OF FACTS

1. This appeal lies at the legal intersection between the venerable law of circumstantial evidence and modern digital evidence. It will decide how, in practice, trial courts will reconcile the two. At the same time, a standard must be set that can apply both to cases where possession of the data in question is an element of the offence charged (as in this appeal) and to cases where it is not.

2. Indeed, the issues go far beyond the factual matrix of this case and must deal with an industry that constantly generates new technology, new services and new types of data. A rational and logical test will evaluate the evidentiary effect of all the evidence and will not be tied to a particular type of data or technology. Digital evidence does not lend itself to closed categories or a rigidly categorized test for proof of the possession of data.

3. For this reason, the Attorney General of British Columbia ("AGBC") submits the test for proof of possession does not require changes to accommodate digital evidence, but rather that the traditional test is the most appropriate as it stood before the erroneous decision of the court below and as previously applied by various trial courts. This test is sufficient flexible and robust to deal with on-going technological changes.

4. Under this approach, it is wrong in law to require the Crown to disprove speculative defences based on mere conjecture and not on evidence. It is equally wrong in law to require the Crown to prove knowledge by proving exclusive access to a data storage device.

5. The AGBC agrees with and adopts the Appellant's overview and statement of facts.

PART II – INTERVENER'S POSITION ON APPEAL

6. The AGBC intervenes to address the analytical framework for the circumstantial proof of possession of digital evidence and to provide practical suggestions for the construction of that framework.

7. *"Issue 1: Where the Crown's evidence is circumstantial, does the rule in Hodge's Case mandate an acquittal where there is an innocent possibility not based in any actual evidence? Put another way, must the Crown disprove all innocent possibilities, whether or not there is any evidence to support them?"* The AGBC submits the Crown is not required to disprove innocent possibilities which are unsupported by evidence.

8. *"Issue 2: Before a case of possession of child pornography can go to a trier of fact, must the Crown prove, beyond any hypothetical possibility, that the accused had exclusive access to the computer throughout the period over which the pornography was downloaded?"* The AGBC submits that while exclusive access to a device can be relevant to proving possession of data on it, it is neither a prerequisite for conviction nor should it be the subject of greater emphasis than other kinds of evidence. The correct test is whether knowledge has been proven beyond a reasonable doubt by relevant and probative evidence.

PART III – STATEMENT OF ARGUMENT

A. The Court Below Fixated on Exclusive Access/Possession to the Exclusion of Other Relevant Factors

9. Exclusive access to the device containing impugned data should be given no greater weight than any other factor. The same reasoning applies to exclusive possession of the device. Such exclusive access/possession, taken in isolation, may be insufficient to prove possession of the data just as the absence of exclusivity may be insufficient to raise a reasonable doubt.

10. The test regarding circumstantial evidence should be the same whether the evidence is digital, physical or testimonial: does the totality of the evidence prove knowledge and control to the requisite standard?

11. The Court below erred and applied a test that emphasized the lack of evidence led by the Crown to prove exclusive access and control to a computer owned by the accused. The ruling also overemphasized "downloading" as the only means by which knowledge of the illicit data may be proven. This is contrary to the reasoning of this Court in *R. v. Morelli*, 2010 SCC 8, [2010] 1 S.C.R. 253:

a. On the issue herein, the majority wrote:

   [32] In applying these principles to the facts of this case, I take care not to be understood to have circumscribed or defined constructive possession of virtual objects. I leave open the possibility, for example, that one could constructively possess a digital file without downloading it to his or her hard drive, using for example a Web-based e-mail account to store illegal material.

   …

b. And more expansively in the dissent:

   [144] The definition of possession advanced by the appellant and adopted by my colleague Fish J. could freeze possession in time and limit it to certain modes of storage and media. As a practical matter, there is little difference between

> exercising control over the hard drive of a computer while on the premises where the computer is located and exercising control over of the on-line space of a Web-based hosted service. Moreover, if, to bring a cache into the scope of possession, the accused were required to have knowledge of how caches work, this would require proof of intent or technical savvy on the part of the accused. As I mentioned above, the requisite *mens rea* will be established at trial if it is shown that the accused willingly took control of the object with full knowledge of its character. In light of the inevitability of technological change, it is important not to needlessly handcuff the courts to a concept of possession that is limited to certain technologies or to current-day computer practices. Control has been the defining feature of possession, not the possibility of finding data files on a hard drive. To adopt downloading as the threshold criterion would be to take a formalistic approach rather than drawing a principled distinction between access and possession. The classical approach to possession, rooted in control, therefore remains the most reliable one. It is the one that is most readily adapted to technological developments and it will not require courts to hear detailed forensic evidence of technological advances on an ongoing basis just to keep up with the times.

B. Circumstantial Digital Evidence Requires Consideration of the Entire Context

12. As is set out below, to properly apply the traditional test to proving possession of data, a number of factors must be considered:

a. Personalized data and accounts;
b. Self-identifying data;
c. Extrinsic evidence;
d. Digital forensic examinations;
e. Joint possession; and
f. Constructive possession.

13. Proving the possession of data has evolved away from simply proving exclusive physical possession of a single physical data container such as a home computer. As illustrated in the cases below, personalized data is now typically contained in “accounts”. Access to that data is controlled by credentials such as passwords, not physical possession of the container itself. Examples of this include social media accounts, webmail, online shopping, online financial accounts and similar. The larger the body of evidence about the on-going use of such accounts; the sounder is the inference of the identity of the user. This is particularly true where personal mobile devices are employed. Access to data can be through any number of devices so long as the person seeking access employs the same credentials.

14. In many instances, evidence proving or disproving possession of the impugned data will not be on the seized device. Evidence of an individual's activity may come from records of that activity from "cloud" or remotely stored data such as saved webmails, social media or online personal commerce. Proof that an individual possessed child pornography on their home computer may come from evidence of temporally proximate use of social media and webmail data, the physical location of which might be anywhere in the world. In such instances, proof of exclusive physical access to a device may be of limited relevance.

15. Possession of data can logically be proven by its personalized nature and content that identify the user. It can also be demonstrated by the timing of other digital activities in close temporal proximity to possession of the data. For example, where the use of the impugned data like child pornography occurs while an individual's webmail and social media accounts, containing information specific to that individual, are simultaneously active on the same device, then it is reasonable to infer that the individual has knowledge of the impugned data. Several case examples illustrate this approach.

16. For example in *R. v. Dhillon*, 2015 BCSC 280, an inference of identity was drawn in part based on the personalized content of the accused's accounts. In a trial for criminal contempt, the following evidence was accepted by the court:

> [57] I note that throughout the session which involved editing the blog and which continued as I will describe, the user operated the user account named "owner" or "Satinder".
>
> [58] Within less than two minutes of completing the edit of the April 2010 blog, the user then logged into two of the "Satinder Dhillon" email accounts by way of webmail, and read and sent or forwarded messages, some of those with content apparently relating to Mr. Dhillon's business or personal interests.
>
> [59] The sequence of events I have just described provides powerful evidence that it was Mr. Dhillon who used the Acer to edit the April 2010 blog. Moreover, on a consideration of Ms. Chau's analysis of the Acer as a whole, there is no evidence to indicate that anyone other than Mr. Dhillon used that computer.

17. Similarly in *R. v. Donnelly,* 2010 BCSC 1294, the accused was on trial for sexual offences, possession of child pornography and breach charges. With respect to the knowledge and control of the child pornography files, the court found:

> [115] The circumstantial evidence with respect to knowledge and control of the child pornography files on the Dell laptop is perhaps even more compelling, in that the use of tattoo[...]@hotmail.com, which I have found was Mr. Donnelly's and was used by him, was between May 25th and June 2, 2008. This brackets the relatively

> narrow period of May 27th and 31st, during which child pornography files were downloaded to the computer.
>
> [116] With respect to the Facebook chat with Kevin Harding on May 31st, it seems to me to be speculative on the available evidence to have a doubt that the person identifying himself as “Ryan Donnelly” was anyone other than Mr. Donnelly, the accused. Further, the proximity in time of his statement about being in “need” to the playing of the video with the title "Really Sexy 12-year-old Gets [DELETED]" is meaningful evidence of his knowledge and control over the child pornography that was found on the laptop, even though that particular video itself is no longer available for analysis.
>
> [117] Similarly, the proximity in time between the downloading from LimeWire of videos with names indicative of child pornography on May 27th and Mr. Donnelly's access to his hotmail and Windows Live Messenger leads to a strong inference of Mr. Donnelly being in charge of all of the downloads, including those of the child pornography files that were found on the computer at the time of forensic analysis.

18. In *R. v. Harris*, 2010 PESC 32, the issue was the circumstantial proof of the use of the contents of a Facebook account alleged to have been owned and used by the accused. The accused took the position the standard had not been met. However, the Court compared the content of the digital evidence to other evidence and rejected the accused’s submission:

> 29 Finally, the theory of the Defence defies logic and common sense. It makes no sense for an unknown third party to impersonate on Facebook Justin Harris, a person whom the complainant has known for most of her life. The futility of such an impersonation is obvious in that the plan for a sexual liaison requires that there eventually be a face-to-face meeting. When the complainant sees that she's dealing with an unknown person, the plan crumbles.
>
> 30 In the final analysis, the Defence invites me to speculate, and I cannot do so. The evidence points to no other rational conclusion then that the accused is the author of 38 e-mails to the complainant and the recipient of 33 e-mails from her between the time period May 24, 2009, and July 24, 2009.

19. The law regarding the proof of possession must be broad enough and flexible enough to account for self-identifying data, the probative value of which is completely independent of the physical location of where it is stored. Self-identifying data means data which contains information indicating who created it. Unlike some physical evidence, certain kinds of data self-identify the person who created them by content, including written content. Emails or other stored digital communications may contain content that identifies the writer irrespective of exclusive access to the device by reference to matters within the unique knowledge of the writer. Similarly digital images and digital video may depict the

accused and be present in sufficient quantity that only the accused would have such a collection.

20. An example of this kind of self-identifying evidence is found in *R. v. Donnelly*:

> [46] Windows Live Messenger is a program for text communication between users that takes place in real time. On this computer, the email address "tattoo[...]@hotmail.com" is shown in the drop-down log-in menu for Windows Live Messenger. This means that a person with that address has used this program. The Windows Live Messenger account requires a password but if the user stays signed on then someone else could use that account without supplying any password. A user of Windows Live Messenger can provide a photograph to accompany his or her address. The photograph accompanying tattoo[...]@hotmail.com at the time that the computer was seized is of Mr. Donnelly, as are the previous pictures that were used for that address.
>
> [48] In the "My Pictures" folder of the computer, there was a sub-folder called "Camera Pics" containing 212 photographs of Mr. Donnelly, Ms. Johnson, the complainants, her other children, their pets and the family engaged in various holiday events.

21. An accused's knowledge of the data may support a finding of possession despite possible access to the physical device by others. The law regarding proof of possession must also account for digital forensics indicating the presence of data demonstrating knowledge irrespective of possible access to the physical device by others. Evidence that data is password protected and then is accessed may be very cogent evidence of possession even if the device passes through many hands. Some accumulated data is beyond even the authorized user's access and cannot be seen or manipulated by an individual. As before, this data is very cogent regardless of who handled the device. The probative value of this kind of evidence is not diminished merely by the fact that other persons may have used the device on which the data resides.

22. In *R. v. Billings*, 2015 ONSC 972, the accused was charged with child pornography offences. The digital forensics expert gave evidence regarding his findings as to who was using the computer which the court accepted:

> [15] According to Det. Villeneuve, there were two Skype accounts that existed on the target computer, but only one that was ever used. One account was in the name of "sgoodwin58". The other account was in the name of "sandy.billings4". The only Skype account that was used on this computer was the "sandy.billings4" account. The profile for the Skype account contained information related to the accused as well as a photo of the accused. Detective Villeneuve testified that there were logs available on the computer of all the Skype calls that were made on the target

> computer. Most of the calls were very short and the chat messaging primarily involved discussions relating to the playing of computer card games.
>
> [16] There was also a MSN Messenger program that was on the computer. Detective Villeneuve indicated that there were three accounts associated with that program, but only one was ever used and it was in the name of "romeo1959@hotmail.com". It was conceded by defence counsel that the accused's middle name is Romeo and he was born in 1959. In addition, the profile information related to the accused.
>
> [17] Finally, Det. Villeneuve told the court that the Internet history showed there were three main types of activity that occurred: (1) searches using terms strongly suggestive of child pornography9, (2) log-ins to Facebook and (3) log-ins to Pogo. He testified that the Pogo site was an Internet gaming site where users could play computer card games with other users. The Internet history revealed that the username associated with access to the Pogo site was "sandyromeo1959".Internet history revealed that the username associated with access to the Pogo site was "sandyromeo1959".
>
> [18] The last analysis that Det. Villeneuve indicated he undertook was to look at the timeline of the Internet searches for what appeared to be child pornography and activity by the "sandy.billings4" Skype account. This analysis revealed that searches occurred regularly and within relatively short periods of time before, during and after Skype activity.
>
> See also *R. v. Dhillon*, paras 41-49, and *R. v. Smith*, 2011 BCSC 1826, paras 119-122

23. In this context, any test for proof of possession of data must account for **joint possession**. Data on a device may be shown to be within both the knowledge and control of more than one individual. In some instances, which individual placed the data on the device, through downloading or any other means will not be relevant. Any number of persons might be shown to both know of the presence of the data and have sufficient control of that data to meet the test for possession. Focus on exclusive physical access to a device will lead to error in such instances. In this regard, the AGBC agrees with and adopts the submissions in paragraphs 89-94 of the Appellant's factum and the authorities cited therein.

24. Similarly, the law must account for **constructive possession** of data. This may occur where data is in another physical location from the individual but where evidence shows that the individual had the requisite knowledge and control irrespective of the location of physical storage for example the contents of a social media account stored in another country. Any test which focuses unduly on exclusive access to a device cannot logically apply to constructive possession of data. It must account for digital evidence on

more than one device and in more than one location to be logically determinative of constructive possession of data. See *R. v. Gilbert*, 2015 NSSC 69, paras 32-34.

25. In many cases a computer will have more than one user and the accused's knowledge and control will be proven by identifying features of the data on the computer, on other devices and from extrinsic evidence such as statements of the accused or witness testimony: see for example *R. v. Allart*, 2012 BCCA 100 at paragraphs 23-24. The totality of the evidence from all sources must be considered and priority should not be given to certain categories of evidence like exclusive physical access to a device or downloading.

26. Fundamentally the court's interest is not in the data itself, but what can inferred about human activity surrounding it as evidenced by use of devices in the creation or manipulation of data. The analysis of data and extrinsic evidence may provide sufficient evidence of such impugned actions to permit the legal inference of possession. Considerations should include but not be limited to:

a. Any evidence of ownership and use of the devices employed to create, use or manipulate data evidencing the impugned actions (traditional extrinsic evidence);
b. The use of any user accounts on the devices;
c. Temporally proximate use of social media accounts, webmails accounts, on-line shopping or access to personal financial or service accounts (Such as Facebook, Twitter, Gmail, Amazon, bank accounts or cellular service accounts) requiring the use of a password, to the impugned actions on the computer;
d. Use of or access to relevant data or accounts from a personalized mobile device (such using the same social media or other accounts from a mobile device as has been shown to be in use on a computer at the same time as the impugned actions);
e. The presence of stored personal information such as emails with personalized content, personal documents or similar evidence (such as word documents, electronic bills, bank statements);
f. The presence of self-identifying data indicating use of the device such as personal digital images or videos (Such as vacation photographs or "selfies");
g. Internet usage identifying a person's activity in temporal proximity to the impugned actions including access to accounts and search terms used;
h. Forensic analysis of the past functions of the devices indicating human use of the machine (as opposed to purely mechanical functions) in temporal proximity to the impugned actions;
i. Personal account information from internet service and cellular service providers indicating who is paying for internet or cellular access;
j. Any "deleted" information indicating past use of the devices relating to the impugned actions; and
k. Any digital signatures employed by users of the devices.

C. Other Appellate Authority Rejects Speculative Inferences

27. The law as reformulated by the Court below regarding circumstantial proof of possession is contrary to recent British Columbia and Ontario appellate authority. These decisions illustrate how other appellate courts have dealt with speculative defences to the possession of data based on circumstantial evidence:

a. *R. v. Bischel*, 2014 BCCA 251:

> [46] With reference to *Griffin* this Court rejected a compelling "possibility" advanced by an appellant in a circumstantial case, finding that it required an untenable interpretation of the evidence in *R. v. Ahmadzai*, 2012 BCCA 215 at para. 35. The possibility of manipulation by an unspecified party raised by Mr. Bichsel in this case is similarly untenable. It is not a rational inference on the evidence, only a mere possibility based on unsubstantiated speculation.

b. *R. v. Midwinter*, 2015 ONCA 150:

> [18] The Agreed Statement of Facts stated that pornographic images were organized into folders and sub-files and that the sub-folders within the Movies folder in which the 781 "total" images were found bore titles which included the words "sexy child". The findings of fact made by the trial judge in his reasons, based upon the Agreed Statement of Facts and the evidence led at trial, included the following:
>
> (i) The prohibited images found on the basement computer were child pornography;
>
> (ii) The appellant was the owner and the primary user of the basement computer, but multiple other users also had access;
>
> (iii) There was no evidence of any remote access to the basement computer;
>
> (iv) The theory that Wendy Midwinter and Trisha Dorman conspired to plant the child pornography images on the appellant's basement computer was "speculative at best";
>
> (v) It was illogical to expect those alleged conspirators would wipe out that which they had allegedly planted for the police to discover in the first place; and,
>
> (vi) The appellant deleted the Movies folder on the evening of September 15, 2009, after learning that the police would visit his home the following day to talk with him.

28. In both of these cases, the Courts upheld the trial decisions and denied appeals based on speculative defences. With any device, it is always "possible" that someone else had access to the device. If this unsupported speculation is sufficient to raise a reasonable doubt, then no conviction may ever result based on digital evidence. Such a speculative and unsubstantiated possibility could not raise a reasonable doubt prior to the advent of computers, and it is illogical and wrong at law to impose such a standard now. If a person is shown to have knowledge and control of the contents of their bedroom, the Crown is not required to prove no one else has ever been in there.

D. Conclusion

29. As the Appellant sets out in paragraph 27 of its factum, the court below focused heavily on points which were not relevant except to disprove speculative and hypothetical possibilities. In the circumstances of this case and cases involving digital evidence generally, this is not a logical formulation of the law of possession. It is largely inconsistent with the law as it has been applied by trial courts as digital evidence has become more common.

30. The AGBC agrees with the Appellant that the only live issue in this case is knowledge and the trial judge correctly instructed himself as to the law before finding the Crown had met its burden. As such, appellate review is not properly available to that finding.

31. The AGBC submits that the traditional test is the most appropriate as it stood before the decision of the court below. As set out above, that test is broad and sophisticated enough that it does not have to be changed to accommodate digital evidence. The Court below by creating circumstantial evidence rules particular to digital evidence has failed to take proper account of reliable and probative evidence to the exclusion of categories which may be of little relevance. It is unnecessary to prove exclusive access to a device in most cases. The AGBC agrees with the Appellant that it is wrong in law to apply the Rule in *Hodge's* case to the knowledge element in this case. It is an error of law to require the Crown to disprove speculative possibilities

PART IV – SUBMISSIONS CONCERNING COSTS

32. The AGBC makes no submissions on costs.

PART V – ORDER SOUGHT

33. The AGBC submits the conviction should be restored and the correct law for the proof of possession restated.

ALL OF WHICH IS RESPECTFULLY SUBMITTED,

_____

Daniel M. Scanlan
Counsel for the Intervener
Attorney General for British Columbia

dated this 4th day of February, 2016
at Victoria, British Columbia

PART VI – TABLE OF AUTHORITIES

Paragraph

PART VII – STATUTES

Criminal Code R.S.C., 1985, c. C-46	*Code criminal* L.R.C. (1985), ch. C-46
Part V – Sexual Offences, Public Morals and Disorderly Conduct	Partie V – Infractions d'ordre sexuel, actes contraires aux bonnes moeurs, indonduite
Definition of *child pornography* **163.1 (1)** In this section, child pornography means (a) a photographic, film, video or other visual representation, whether or not it was made by electronic or mechanical means, (i) that shows a person who is or is depicted as being under the age of eighteen years and is engaged in or is depicted as engaged in explicit sexual activity, or (ii) the dominant characteristic of which is the depiction, for a sexual purpose, of a sexual organ or the anal region of a person under the age of eighteen years; (b) any written material, visual representation or audio recording that advocates or counsels sexual activity with a person under the age of eighteen years that would be an offence under this Act; (c) any written material whose dominant characteristic is the description, for a sexual purpose, of sexual activity with a person under the age of eighteen years that would be an offence under this Act; or (d) any audio recording that has as its dominant characteristic the description, presentation or representation, for a sexual purpose, of sexual activity with a person under the age of eighteen years that would be an offence under this Act.	**Définition de *pornographie juvénile*** **163.1 (1)** Au présent article, pornographie juvénile s'entend, selon le cas : a) de toute représentation photographique, filmée, vidéo ou autre, réalisée ou non par des moyens mécaniques ou électroniques : (i) soit où figure une personne âgée de moins de dix-huit ans ou présentée comme telle et se livrant ou présentée comme se livrant à une activité sexuelle explicite, (ii) soit dont la caractéristique dominante est la représentation, dans un but sexuel, d'organes sexuels ou de la région anale d'une personne âgée de moins de dix-huit ans; b) de tout écrit, de toute représentation ou de tout enregistrement sonore qui préconise ou conseille une activité sexuelle avec une personne âgée de moins de dix-huit ans qui constituerait une infraction à la pré- sente loi; c) de tout écrit dont la caractéristique dominante est la description, dans un but sexuel, d'une activité sexuelle avec une personne âgée de moins de dix-huit ans qui constituerait une infraction à la présente loi; d) de tout enregistrement sonore dont la caractéristique dominante est la description, la présentation ou la simulation, dans un but sexuel, d'une activité sexuelle avec une personne âgée de moins de dix-huit ans qui constituerait une infraction à la présente loi.
Making child pornography **(2)** Every person who makes, prints, publishes or possesses for the purpose of publication any child pornography is guilty of an indictable offence and liable to imprisonment for a term of not more than 14 years and to a minimum punishment of	**Production de pornographie juvenile** **(2)** Quiconque produit, imprime ou publie, ou a en sa possession en vue de la publication, de la pornographie juvénile est coupable d'un acte criminel passible d'un emprisonnement maximal de quatorze ans, la peine minimale étant de un an.

imprisonment for a term of one year.	
Distribution, etc. of child pornography **(3)** Every person who transmits, makes available, distributes, sells, advertises, imports, exports or possesses for the purpose of transmission, making available, distribution, sale, advertising or exportation any child pornography is guilty of an indictable offence and liable to imprisonment for a term of not more than 14 years and to a minimum punishment of imprisonment for a term of one year.	**Distribution de pornographie juvenile** **(3)** Quiconque transmet, rend accessible, distribue, vend, importe ou exporte de la pornographie juvénile ou en fait la publicité, ou en a en sa possession en vue de la transmettre, de la rendre accessible, de la distribuer, de la vendre, de l'exporter ou d'en faire la publicité, est coupable d'un acte criminel passible d'un emprisonnement maximal de quatorze ans, la peine minimale étant de un an.
Possession of child pornography **(4)** Every person who possesses any child pornography is guilty of (a) an indictable offence and is liable to imprisonment for a term of not more than 10 years and to a minimum punishment of imprisonment for a term of one year; or (b) an offence punishable on summary conviction and is liable to imprisonment for a term of not more than two years less a day and to a minimum punishment of imprisonment for a term of six months.	**Possession de pornographie juvenile** **(4)** Quiconque a en sa possession de la pornographie juvénile est coupable : a) soit d'un acte criminel passible d'un emprisonnement maximal de dix ans, la peine minimale étant de un an; b) soit d'une infraction punissable sur déclaration de culpabilité par procédure sommaire et passible d'un emprisonnement maximal de deux ans moins un jour, la peine minimale étant de six mois.
Accessing child pornography **(4.1)** Every person who accesses any child pornography is guilty of (a) an indictable offence and is liable to imprisonment for a term of not more than 10 years and to a minimum punishment of imprisonment for a term of one year; or (b) an offence punishable on summary conviction and is liable to imprisonment for a term of not more than two years less a day and to a minimum punishment of imprisonment for a term of six months.	**Accès à la pornographie juvenile** **(4.1)** Quiconque accède à de la pornographie juvénile est coupable : a) soit d'un acte criminel passible d'un emprisonnement maximal de dix ans, la peine minimale étant de un an; b) soit d'une infraction punissable sur déclaration de culpabilité par procédure sommaire et passible d'un emprisonnement maximal de deux ans moins un jour, la peine minimale étant de six mois.
Interpretation **(4.2)** For the purposes of subsection (4.1), a person accesses child pornography who knowingly causes child pornography to be viewed by, or transmitted to, himself or herself.	**Interprétation** **(4.2)** Pour l'application du paragraphe (4.1), accède à de la pornographie juvénile quiconque, sciemment, agit de manière à en regarder ou fait en sorte que lui en soit transmise.

Aggravating factor **(4.3)** If a person is convicted of an offence under this section, the court that imposes the sentence shall consider as an aggravating factor the fact that the person committed the offence with intent to make a profit.	**Circonstance aggravante** **(4.3)** Le tribunal qui détermine la peine à infliger à une personne déclarée coupable d'infraction au présent article est tenu de considérer comme circonstance aggravante le fait que cette personne a commis l'infraction dans le dessein de réaliser un profit.
Defence **(5)** It is not a defence to a charge under subsection (2) in respect of a visual representation that the accused believed that a person shown in the representation that is alleged to constitute child pornography was or was depicted as being eighteen years of age or more unless the accused took all reasonable steps to ascertain the age of that person and took all reasonable steps to ensure that, where the person was eighteen years of age or more, the representation did not depict that person as being under the age of eighteen years.	**Moyen de défense** **(5)** Le fait pour l'accusé de croire qu'une personne figurant dans une représentation qui constituerait de la pornographie juvénile était âgée d'au moins dix-huit ans ou était présentée comme telle ne constitue un moyen de dé- fense contre une accusation portée sous le régime du paragraphe (2) que s'il a pris toutes les mesures raisonnables, d'une part, pour s'assurer qu'elle avait bien cet âge et, d'autre part, pour veiller à ce qu'elle ne soit pas présentée comme une personne de moins de dix-huit ans.
Defence **(6)** No person shall be convicted of an offence under this section if the act that is alleged to constitute the offence (a) has a legitimate purpose related to the administration of justice or to science, medicine, education or art; and (b) does not pose an undue risk of harm to persons under the age of eighteen years.	**Moyen de défense** **(6)** Nul ne peut être déclaré coupable d'une infraction au présent article si les actes qui constitueraient l'infraction : a) ont un but légitime lié à l'administration de la justice, à la science, à la médecine, à l'éducation ou aux arts; b) ne posent pas de risque indu pour les personnes âgées de moins de dix-huit ans.
Question of law **(7)** For greater certainty, for the purposes of this section, it is a question of law whether any written material, visual representation or audio recording advocates or counsels sexual activity with a person under the age of eighteen years that would be an offence under this Act.	**Question de droit** **(7)** Il est entendu, pour l'application du présent article, que la question de savoir si un écrit, une representation ou un enregistrement sonore préconise ou conseille une activité sexuelle avec une personne âgée de moins de dixhuit ans qui constituerait une infraction à la présente loi constitue une question de droit.
1993, c. 46, s. 2; 2002, c. 13, s. 5; 2005, c. 32, s. 7; 2012, c. 1, s. 17; 2015, c. 23, s. 7.	1993, ch. 46, art. 2; 2002, ch. 13, art. 5; 2005, ch. 32, art. 7; 2012, ch. 1, art. 17; 2015, ch. 23, art. 7.