Resolutions Adopted at the 111th Annual Conference

August, 2016

Ottawa, Ontario

CANADIAN ASSOCIATION OF CHIEFS OF POLICE

Safety and security for all Canadians through innovative police leadership

Unit 100 – 300 Terry Fox Drive, Kanata Ontario K2K 0E3
p: 613-595-1101 f: 613-383-0372
e: cacp@cacp.ca w: www.cacp.ca

Table of Contents

Resolution #01 - 2016

RESOLUTION FOR THE SUPPORT OF A COMPETENCY-BASED HUMAN RESOURCE FRAMEWORK FOR CANADIAN POLICE SERVICES

Submitted by the Human Resources and Learning Committee

WHEREAS the CACP Human Resources and Learning Committee has recognized the immense value of the competency-based management framework, and;

WHEREAS the Province of British Columbia has recognized the value of competency-based training and in 2010 strongly recommended that all municipal police recruits be trained using curriculum that is mapped to the Police Sector Council competencies, and;

WHEREAS the Alberta Association of Chiefs of Police resolved calling for the Government of Canada, through Public Safety Canada, to provide the necessary funding to support the on-going accessibility and ever-greening, of the CBMF, and:

WHEREAS the Ontario Association of Chiefs of Police resolved at its 64th Annual General Meeting in June, 2015 to encourage and support the use of CBMF by Ontario's police services, and;

WHEREAS police services and employees across Canada access the CBMF materials daily to assist in training, succession management, executive development, promotional process, talent management, learning plans, and performance management, and;

WHEREAS we all, in policing, have invested significantly in its development and have a vested interested in ensuring the CBMF continues to be available, accessible, implemented and maintained.

THEREFORE BE IT RESOLVED that the Canadian Association of Chiefs of Police calls on the Government of Canada (Public Safety Canada) to provide the necessary funding for the on-going accessibility and updating of the CBMF.

Resolution #01 - 2016

RESOLUTION FOR THE SUPPORT OF A COMPETENCY-BASED HUMAN RESOURCE FRAMEWORK FOR CANADIAN POLICE SERVICES

Background

Over the past nine years, the Police Sector Council, funded by the Government of Canada, undertook the development of a Competency-based HR Management Framework (CBMF) to improve and enhance HR management and police professionalism.

Working under a mandate to provide innovative, practical solutions to HR planning and management challenges in the Canadian policing sector, the Police Sector Council undertook this development of a CBMF over a five year period with $11M in federal government investment and countless hours of in-kind support and input from Canadian police services, individuals, partners, and stakeholders. The Framework is based on research and best practices in Canada and internationally. It details competency-based processes, profiles, tools, and templates for 33 police roles in the areas of general duty, investigation, and leadership/management.

Given the investment of time, money, and resources, there is a clear demand for a competency-based approach to HR management in the Canadian police sector. As a cornerstone to the larger issue of professionalization, the CBMF contributes to workforce management, career planning, labour mobility, the defensibility of police actions, and will generate other economic efficiencies associated with the adoption of common training standards. In addition to the work taking place in British Columbia for police recruit training, 8 of the 13 police training academies are assessing the CBMF to develop, refine, or re-design their curriculums to align to the national framework. Numerous police services are using the CBMF as a tool to improve the way they manage staff and resources at all levels.

In April 2013, the Police Sector Council was dissolved due to lack of funding. In 2015, the Framework and the associated policing Intellectual Property was “gifted” to the Canadian Police Knowledge Network (CPKN). CPKN now oversees the administration and stewardship of the Framework on behalf of the police community, primarily protecting the CBMF intellectual property through controlled access. Since 2015, 144 individuals from 75 police services and related agencies have been granted access to the CBMF.

The CBMF and its associated materials are not static resources. They must be regularly reviewed and updated, or ever-greened, to ensure they align to evolving practices in the policing sector and are able to support the development of consistent training and practice in policing over the long-term. Not to do so puts both the original investment and knowledge inventory at risk. To date, both the Ontario Association of Chiefs of Police and the Alberta Association of Chiefs of Police have adopted resolutions calling for the Government of Canada, through Public Safety Canada, to provide the necessary funding to support the on-going accessibility and ever-greening, of the CBMF.

This significant investment of time, effort, and funding by government and many in policing resulted in national occupational standards and readily available, practical and valuable materials to improve the way we manage staff and resources at all levels. Funding is now required to review and update the CBMF, as CPKN does not have the infrastructure or the financial resources to do this.

Resolution #02 - 2016

CHILD PHYSICAL ABUSE IMAGERY

Submitted by the Law Amendments Committee

WHEREAS there is a proliferation of online material depicting the physical abuse of children, and;

WHEREAS child physical abuse imagery violates the dignity, rights and privacy of a victimized child and signals there may be a child in dire need of protection, and;

WHEREAS there are provisions aimed at eliminating child pornography in the *Criminal Code*, no such provisions exist to adequately prohibit the public posting of child physical abuse imagery on the internet, and;

WHEREAS the absence of clear criminal prohibitions render it difficult to investigate or remove child abuse imagery on the Internet, and critically, impossible to identify and apprehend those individuals actively engaged in such harmful activities.

THEREFORE BE IT RESOLVED that the Canadian Association of Chiefs of Police urge the Government of Canada to protect children by amending the *Criminal Code* to prohibit the making and posting of child abuse imagery as well as mandating the removal and deletion of such images from the Internet.

Resolution #02 - 2016

CHILD PHYSICAL ABUSE IMAGERY

Background

As will be described below, this proposal contains two options for the Government of Canada to consider in amending the *Criminal Code* to prohibit the making and posting of child abuse imagery as well as mandating the removal and deletion of such images from the Internet. (*See **Appendix "A"** for a more detailed analysis of this proposal- available in English only*).

Making and Posting

The public posting of child physical abuse imagery has emerged as a concerning trend on the Internet. Moreover, child physical abuse imagery violates the dignity, rights and privacy of a victimized child, and also signals there is likely a child in dire need of protection. Posts may include gratuitous violence against a child and verbal abuse that violates the dignity of the child. In order to protect the child from the existing and future harm of the imagery, or continued physical harm, an investigation is required. Without an investigation, an offender cannot be identified and the child cannot be protected from ongoing and future physical abuse. Moreover, content networks and providers are key to advancing an investigation. As posting child physical abuse imagery is not currently illegal, content networks are currently exempt from providing the necessary information to law enforcement and have discretion in determining what, if any, action that they choose to take.

Removal Provisions

Child physical abuse imagery traumatizes the public and is of grave concern. The nature of the content depicted in some videos posted to the Internet can be so horrific that it leaves an unwitting viewer shocked and disturbed. The removal of child physical abuse content is critical to mitigate the continued harm caused to both the child and to the public. The imagery may be degrading and private to the child, the public may be disturbed, shocked and desensitized when viewing the content, and it is for such reasons that a removal mechanism is critical.

Content providers are key to preventing the further posting and spread of child physical abuse imagery. They can block users, posts and imagery and allow for the easy reporting of content, detect patterns, educate users and create internal policies to support their objectives. Currently, content providers are generally private entities that only remove illegal content once it is brought to their attention by users or where there is a court order. However, since child abuse imagery is not illegal, there is currently no way to compel its removal from their network.

Jurisdiction

Child physical abuse imagery on the Internet also poses jurisdictional challenges. First, currently no one agency in Canada has the responsibility or mandate for dealing with this imagery posted on the Internet. Host jurisdictions may or may not have mutual enforcement agreements to uphold Canadian court orders regarding such requests for information or removal of data.

However, where another country is cooperative with Canadian authorities it would likely need to be pursuant to a court order and so the current lack of prohibition and removal authority precludes this option.

Proposal:

For the purposes of this proposal, a definition of child physical abuse imagery in the *Criminal Code* will be required and ought to be sufficiently narrow to capture the intent of the proposed prohibition and to eliminate the public posting of child abuse imagery on the Internet. Currently Part V of the *Criminal Code*, contains several sections that are similar in nature to the proposed child abuse imagery prohibition. However, none of these sections adequately capture what is required to prohibit the public posting of child abuse imagery on the Internet and as such would need modifications, such as:

Option #1: Addition of a New Subsection of Section 163

In the first scenario, a new subsection of section 163 would be created to address the core definition of child abuse imagery and what acts are prohibited with respect to child abuse imagery. This would be specifically tailored for a narrow focus of the prohibition of publicly posting child abuse imagery on the Internet. Because it would be a section 163 offence, the existing relevant punishment section (section 169) would not need to be amended. However, section 164 would be required to be amended to include "child abuse imagery" in its removal authorities.

A child abuse imagery subsection in section 163 could be properly placed as "section 163(2.1)":

> **163**(***2.1***) ***Child Physical Abuse Imagery***
>
> ***Every one commits an offence who publishes, makes public or transmits for the purpose of making publicly available or publishing, a photographic, film, video, audio or other audio or visual representation, 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 being subjected to explicit acts of violence or abuse.***

** Note that the above proposed amendment is based on the wording of section 163(1) and section 162.1 but tailored for the narrow purpose of prohibiting public posting of child abuse imagery on the Internet.**

Option #2: New "Deeming" Provision

A second scenario would be to include a new subsection that *deems* child physical abuse imagery as a form of "obscenity" that falls within the existing framework of section 163(1) and (2). This option would use the existing language of sections 163(1) and (2) to capture the act of publicly posting child abuse imagery on the Internet.

Conclusion

Child abuse is a pressing issue in society and children have been afforded special protection in society by virtue of their inherent vulnerabilities and dependence. A relatively new issue of child abuse imagery posting on the Internet has arisen and carries a real risk of re-victimizing children while traumatizing and desensitizing the unwitting public. Such online posts to some may have the effect of normalizing, promoting or encouraging child abuse.

As is often the case, Internet technology and its social utility have surpassed the development of the law and prevent law enforcement from carrying out its mandate to investigate such matters. Posted child abuse imagery is analogous to a physical poster or TV advertisement showing real child abuse. The community would agree that such a practice would be abhorrent and offensive to the community standards of tolerance. However, this conduct is currently permitted online despite the Internet's reach being much greater than any advertisement or physical poster.

To remedy the public Internet posting of child physical abuse imagery the law must prohibit the conduct and provide the commensurate methods of investigation and removal. This can be facilitated through amending the *Criminal Code* to create a new section to prohibit Internet posting or deem child abuse imagery as obscene while amending the existing removal provisions to include child abuse imagery.

Appendix "A"

Resolution #02 - 2016

CHILD PHYSICAL ABUSE IMAGERY

The public posting of child physical abuse imagery has emerged as a concerning trend on the Internet. In 2014, the Canadian Centre for Child Protection (C3P) prepared a report on the live recording of child physical abuse and its posting to the Internet.[1] In the course of operating Cybertip.ca, the C3P and its staff have been exposed to an alarming continuum of child abuse imagery ranging from advocating harming children to the live recording of violence against children.[2] The C3P report respectively designates the ends of the continuum as ranging from "concerning content" on the low end of severity to "extremely concerning content" on the high end of severity. The report defines "concerning content" as where the child may be in need of protection and "extremely concerning content" depicting a criminal offence and violating the child's dignity and privacy.

The C3P report identified the central issue of child abuse imagery to be that Canada (nor any other nation) neither prohibits the recording, sharing or posting of child physical abuse nor compels its removal from Internet content networks (e.g. Facebook, Twitter, Instagram, YouTube, etc.). The following is a summary of the key points of the C3P's report as they relate to this research.

Effect on the Child

Child physical abuse imagery violates the dignity, rights and privacy of a victimized child. It also signals there is a child in dire need of protection. Posts may include gratuitous violence against a child and verbal abuse that violates the dignity of the child. The C3P compared the court's willingness to grant publication bans for cases of child abuse and exploitation to protect their identities and prevent humiliation as a matter of commonly accepted public interest to the lack of regulation on the Internet. A child compromised in an abusive post could be readily identifiable which represents a serious concern to that child's privacy rights and mental wellbeing. In order to protect the child from the existing and future harm of the imagery, or continued physical harm, an investigation is required.

Powers of Investigation

Without an investigation, an offender cannot be identified and the child cannot be protected from ongoing and future physical abuse. Moreover, content networks and providers are key to advancing an investigation. For an Internet investigation to proceed, the investigating agency must be able to access information that can assist in locating the jurisdiction of the post to identify the child and offender. As posting child physical abuse imagery is not currently illegal,

[1] Canadian Centre for Child Protection, *Child Abuse Recorded Via Technology ("Recording Live Child Abuse")* (May 6 2014) (the report).
[2] *Ibid.*

content networks are currently exempt from providing the necessary information to law enforcement and have discretion in determining what, if any, action that they choose to take. Where a content provider refuses to provide information such as the posting party's Internet Protocol (IP) address, date of the post or other relevant information regarding the posting party, the investigation may not advance. Obtaining an IP address is critical to this type of Internet investigation because it allows an Internet subscriber to be identified through their Internet Service Provider (commonly called ISP). This requires investigative authority such as a *Criminal Code* prohibition, as there is with intimate images as well as child pornography. This permits the police to obtain the court order necessary to identify the person behind an IP address who may be, or be able to identify, the posting party.

A further concern is related to the law enforcement agency conducting the investigation, as well as the degree of cooperation from content and ISP providers. For instance, a content provider may be more willing to provide police information than to child protection services. ISP's require that investigative agencies have a court order to obtain the name and particulars associated to an IP address (tombstone information), which child protection agencies may be unable to get under their enabling statute.[3]

Effect on the Public

Child physical abuse imagery traumatizes the public and is of grave concern to the C3P. The nature of the content depicted in some videos posted to the Internet can be so horrific that it leaves an unwitting viewer shocked and disturbed. For this reason, staff at Cybertip.ca often mute the volume of suspected child physical abuse imagery when reviewing it. Unsuspecting members of the public often do not have this foresight when accessing content on social media and other Internet networks, which inevitably causes the exposure to traumatic and disturbing material.

The C3P is also concerned that repeated exposure to child physical abuse imagery on the Internet can cause certain populations to become desensitized and even possibly adopt ideas that physically abusing children is acceptable, or normal, in society. Once this imagery is posted, it can be viewed anywhere, commented on, shared, forwarded, saved and re-posted on different content networks. The ease of sharing content and its global may de-sensitize the public by the repeated bombardment of child abuse imagery. Ultimately, this may lead to a change in societal norms and an increase in the prevalence of child abuse.

Removal and Prevention

The removal of child physical abuse content is critical to mitigate the continued harm caused to both the child and to the public. The imagery may be degrading and private to the child, the public may be disturbed, shocked and desensitized when viewing the content, and it is for such reasons that a removal mechanism is critical.

Content providers are key to preventing the further posting and spread of child physical abuse

[3] More discussion on the role of child protection agencies in relation to this issue is necessary.

imagery. They can block users, posts and imagery and allow for the easy reporting of content, detect patterns, educate users and create internal policies to support their objectives. Currently, content providers are generally private entities that only remove illegal content once it is brought to their attention by users or where there is a court order. However, since child abuse imagery is not illegal, there is currently no way to compel its removal from their network. This permits a content provider to exercise discretion whether or not to remove the content. If a provider decides not to remove content, there is no legal recourse to compel them to do so. Thus, a prohibition and removal authority is required to compel the removal of child physical abuse imagery.

Jurisdictional Issues

Child physical abuse imagery on the Internet also poses jurisdictional challenges. First, currently no one agency in Canada has the responsibility or mandate for dealing with this imagery posted on the Internet. The C3P refers to this as a "jurisdiction vacuum" where concerned members of the public do not know who to report content to, or what action to take. The result is that the information could be sent from agency to agency, reporting may occur to multiple agencies or no report is made to as the reporting person is unsure as to where to go. Critical witness information may be lost or never reported while investigative efforts could be inefficiently duplicated across jurisdictions and agencies.

Moreover, many of the major public Internet content providers are located outside of Canada. Both the data of the content provider and the provider's corporate offices may be abroad and therefore outside the direct reach of Canadian police or child protection agencies and courts. The data servers may even have redundant copies in multiple jurisdictions and the content may be subject to conflicting laws of the host jurisdictions. Host jurisdictions may or may not have mutual enforcement agreements to uphold Canadian court orders regarding such requests for information or removal of data. However, where another country is cooperative with Canadian authorities it would likely need to be pursuant to a court order and so the current lack of prohibition and removal authority precludes this option.

Working Definition of "Child Physical Abuse Imagery"

For the purposes of this proposal, a definition of child physical abuse imagery will be required and ought to be sufficiently narrow to capture the intent of the proposed prohibition and to eliminate the public posting of child abuse imagery on the Internet. Any proposed provisions must ensure that only this area is prohibited and the offence and removal provisions do not extend to any purposes for public good such as mainstream media or awareness/educational materials that may be publicized online.

Similar Provisions in Effect

Currently Part V of the *Criminal Code*, contains several sections that are similar in nature to the proposed child abuse imagery prohibition. However, none of these sections adequately capture

what is required to prohibit the public posting of child abuse imagery on the Internet. A summary of the similar provisions as the current state of the law follow below.

Under *Sexual Offences*, section 162.1 deals with publication of an intimate image without consent. Section 162.1(1) specifically prohibits the knowing publishing, transmission, sale, making available or advertisement of intimate images without the consent of the person depicted. Section 162.1(2) defines "intimate image" as a visual recording of a person made by any means including a photographic, film or video recording that depicts nudity, genitals, breasts, sexual activities and where there was a reasonable expectation of privacy at the time the image was taken and that existed at the time of the offence. Section 162.2(1) allows the court to prohibit an offender from using the Internet or other digital network unless the offender complies with conditions set by the court.

Under *Offences Tending to Corrupt Morals*, section 163(1) prohibits the making, printing, publishing, distributing or possession for the purpose thereof of any obscene written material, picture, model, phonograph record or other thing. Section 163(2)(a) further prohibits the knowing sale, exposure of possession for the purpose thereof of the items listed in section 163(1). Section 163(2)(b) prohibits the knowing public exhibition of a disgusting object or indecent show.

Section 163.1 deals with child pornography and defines it and prohibits making, distributing, possessing, and accessing child pornography. Child pornography is defined, in part, as relating to persons under the age of 18. Section 163.1 also provides a framework as to what constitutes a recording and includes audio representations.

Section 164.1, deals with the court's authority over images depicting child pornography, advertising of sexual services, voyeuristic recordings, obscene imagery and intimate images. Section 164.1(1) authorizes the court to order a warrant that causes the data to be removed from a computer system, a copy provided to the court and any information relating to the identity or location of the person who posted the material provided. Under section 164.1(5), the court may order the data deleted from a computer system.

Options

1. **Addition of a New Subsection of Section 163**

In the first scenario, a new subsection of section 163 would be created to address the core definition of child abuse imagery and what acts are prohibited with respect to child abuse imagery. This would be specifically tailored for a narrow focus of the prohibition of publicly posting child abuse imagery on the Internet. Because it would be a section 163 offence, the existing relevant punishment section (section 169) would not need to be amended. However, section 164 would be required to be amended to include "child abuse imagery" in its removal authorities. A child abuse imagery subsection in section 163 could be properly placed as "section 163(2.1)":

163(***2.1***) ***Child Physical Abuse Imagery***

Every one commits an offence who publishes, makes public or transmits for the purpose of making publicly available or publishing, a photographic, film, video, audio or other audio or visual representation, 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 being subjected to explicit acts of violence or abuse.

Note that the above proposed amendment is based on the wording of section 163(1) and section 162.1 but tailored for the narrow purpose of prohibiting public posting of child abuse imagery on the Internet.

2. New "Deeming" Provision

A second scenario would be to include a new subsection that deems child physical abuse imagery as a form of obscenity that falls within the existing framework of section 163(1) and (2). This option would use the existing language of sections 163(1) and (2) to capture the act of publicly posting child abuse imagery on the Internet. However, this option would also prohibit acts related to child abuse imagery such as private distributing or circulating as well as acts that take place apart from the Internet. The existing prohibitions in these sections would cause the child abuse imagery prohibition to extend to non-Internet based activities such as paper circulation.

Adding express provisions that address the Internet could exceed the scope of addressing child abuse imagery by adding more provisions to section 163(1). "Transmitting" could fall under the existing language of, among other acts, "distributing" or "circulating". Or, by adding "transmitting for a public purpose" the scope of the prohibition could be appropriately narrowed to Internet and technology specific language and minimally interferes with the existing acts under sections 163(1) and (2).

In this scenario, the *Butler* test might apply to the extent that only undue child abuse imagery would be considered obscene notwithstanding any internal necessities ("artistic defence"), in relation to "public good" (e.g. where a citizen records an adult physically abusing a child for the purposes of reporting that adult), and to the extent the community tolerates the material.[4]

This scenario is addressed in the following proposed amendment to section 163(1) and (2) and a new deeming provision based on section 163(8) could be properly added as "section 163(9)" (changes emphasized):

163. **Corrupting morals**

(1) Every one commits an offence who

(a) makes, prints, publishes, distributes, circulates, ***transmits for a public purpose,*** or has in his possession for the purpose of publication, distribution or

[4] *Supra,* note 0.

circulation any obscene written matter, picture, model, phonograph record or other thing whatever; …

(2) Every one commits an offence who knowingly, without lawful justification or excuse,
(a) sells, exposes to public view, ***transmits for a public purpose,*** or has in his possession for such a purpose any obscene written matter, picture, model, phonograph record or other thing whatever; …

163*(9)* Obscene publication ***of child abuse imagery***

For the purposes of this Act, any ***obscene*** publication a dominant characteristic of which is ***the photographic, film, video, audio or, other audio or visual representation, that shows a person who is or is depicted as being under the age of eighteen years and is subjected to or is depicted as subjected to explicit acts of violence or abuse***, shall be deemed to be obscene.

Both proposed scenarios incorporate audio recordings that may disturbingly capture child abuse. This is similar to the child pornography provision in section 163.1. It was further noted in the Canadian Centre for Child Protection report that staff are required to watch videos on "mute" because of how disturbing the audio can be.[5] These factors strongly suggest audio should be included in the prohibition of publicly posting child abuse imagery on the Internet.

Child Pornography Provisions

Section 163.1 is a useful starting point for the definition of child abuse imagery but for the reasons explained below, likely not an appropriate location to place child physical abuse imagery provisions.

Section 163.1(1)(a) defines child pornography as a photographic, film, video or other visual representation made by electronic or mechanical means.[6] Under this subsection, the person depicted must also be under 18 years of age and engaged or depicted in a sexually explicit activity or for a dominantly sexual purpose. Subsection (d) deals with audio recordings that serve to present or represent sexually explicit activities of persons under 18 years of age.

Section 163.1(1) is a helpful basis for the prohibition of child abuse imagery. Child pornography involves many of the same factors as child abuse imagery because both visually and audibly record the abuse of children through degrading and criminal acts. Therefore, section 163.1(1) is an appropriate starting point when drafting a new section for child abuse imagery. The definition of what matter constitutes child pornography can easily be adapted to meet child abuse imagery by changing section 163.1(1) in the following way (changes emphasized):

[5] *Supra*, note 3.
[6] Section 163.1 contains other provisions related to descriptive written representations, counselling the distribution of, making, accessing and possessing child pornography. However, these sections are not relevant to this research as they do not meet the objectives of prohibiting the posting of child abuse imagery.

In this section, "***child physical abuse imagery***" means

> (a) a photographic, film, video***, audio*** or***,*** other ***audio or*** visual representation, that shows a person who is or is depicted as being under the age of eighteen years and is subjected to or is depicted as subjected to explicit ***acts of violence or abuse***, …

With respect to section 163(1)(b), the inclusion of audio within child abuse imagery may be prudent given the potential for graphic audio to be posted on the Internet or for video graphics to be marginally blurred out or hidden to circumvent provisions prohibiting child abuse imagery yet still suggest child abuse.

Section 163.1(3) prohibits the distribution of child pornography which includes transmission, making available, distributing, selling, advertising, importing, exporting or possession for these purposes. The intent of section 163.1(3) is to totally prohibit the movement of child pornography which is typically an underground activity on the Internet. This differs from the posting of child abuse imagery because the content is openly and publicly posted and the private distribution of the content is not illegal in and of itself. Nor is it the intention of the proposed prohibition to necessarily prohibit the private distribution or transmission of child abuse imagery. The issue is the public posting of such child abuse imagery because posting the imagery causes harm to the victim and public desensitization to the issue. Although private transmission or distribution is without a doubt immoral, it exceeds the scope of the proposed criminal prohibition and also is more appropriate dealt with under section 163.

Removal Provisions

The removal and deletion provisions of section 164 can address the inclusion of child abuse imagery provisions into the *Criminal Code* in one of two ways.

Scenario 1 – New Subsection

In the first scenario described above, a new section would be added after section 163(2), “section 163(2.1)” that specifically defines the child abuse imagery offences. Accordingly, section 164 would be amended to include “child abuse imagery” into each of the provisions in the subsections handling removal, deletion and corollary issues. Section 164 was amended in this regard in 2014 to incorporate intimate images. For child abuse imagery, section 164 could be amended in the following way (changed emphasized):

> **(1) Warrant of seizure**
> If a judge is satisfied by information on oath that there are reasonable grounds to believe that there is material — namely, child pornography as defined in section 163.1, ***child physical abuse imagery as defined in section 163(2.1)***, a voyeuristic recording, an intimate image or an advertisement of sexual services as defined in 164(8) or computer data as defined in subsection 342.1(2) that makes child pornography, ***child physical abuse imagery***, a voyeuristic recording, an intimate image or an advertisement of sexual services available — that is stored on and made available through a computer system as

defined in subsection 342.1(2) that is within the jurisdiction of the court, the judge may order the custodian of the computer system to

(a) give an electronic copy of the material to the court;

(b) ensure that the material is no longer stored on and made available through the computer system; and

(c) provide the information necessary to identify and locate the person who posted the material.

(5) Order

If the court is satisfied, on a balance of probabilities, that the material is child pornography as defined in section 163.1, ***child physical abuse imagery as defined in section 163(2.1)***, a voyeuristic recording, an intimate image or an advertisement of sexual services as defined in subsection 164(8) or computer data as defined in subsection 342.1(2) that makes child pornography, ***child physical abuse imagery***, the voyeuristic recording, the intimate image or the advertisement of sexual services available, it may order the custodian of the computer system to delete the material.

(7) Return of material

If the court is not satisfied that the material is child pornography as defined in 163.1, ***child physical abuse imagery as defined in section 163(2.1)***, a voyeuristic recording, an intimate image or an advertisement of sexual services as defined in subsection 164(8) or computer data as defined in subsection 342.1(2) that makes child pornography, ***child physical abuse imagery***, the voyeuristic recording, the intimate image or the advertisement of sexual services available, the court shall order that the electronic copy be returned to the custodian of the computer system and terminate the order under paragraph (1)(b).

Scenario 2 – New Deeming Provision

In the second scenario, child abuse imagery would be incorporated into a new section, section "163(9)" as a deeming provision for a second form of obscenity. In this scenario, no changes are required in section 164 because "obscenity" is included in the existing provisions that provide for the removal of digital content from computer systems that service the Internet or where people can publish imagery. These sections also include intimate images, child pornography and voyeuristic recordings and can appropriately effect the removal of child abuse imagery.

Conclusion

Within the current framework of the *Criminal Code*, two amendment scenarios arise for incorporating a prohibition of the public posting of child abuse imagery on the Internet. In the first scenario, a provision under section 163 would be added and create a new offence of publicly posting child abuse imagery on the Internet. This option requires a new subsection in 163 to be created and section 164 to be amended to include child abuse imagery.

In the second scenario, a provision would be added within the existing structure of section 163 to *deem* child abuse imagery as obscene. In this case, section 164 would not have to be amended. However, this option would fall under the existing structure of section 163(1) and 163(2) which prohibits a wide range of acts such as distributing, circulating, making and possession for the purpose of these acts. Adopting the child abuse imagery provision under these sections could cause the aims of the prohibition of public posting of child abuse imagery on the internet to be exceeded and might run the risk of being considered overbroad and therefore unconstitutional.

Whatever scenario is pursued, effective offender management could be obtained by adopting a section 162.2(1) like provision that enables the court to prohibit or impose conditions on those found guilty of publicly posting child imagery. Depending on the scenario pursued, further work may be required to develop a definition that appropriately captures the goals of the child abuse imagery prohibition and ensure the definition is precise enough to accomplish its aims and not overbroad.

Child abuse is a pressing issue in society and children have been afforded special protection in society by virtue of their inherent vulnerabilities and dependence. A relatively new issue of child abuse imagery posting on the Internet has arisen and carries a real risk of re-victimizing children while traumatizing and desensitizing the unwitting public. Such online posts to some may have the effect of normalizing, promoting or encouraging child abuse.

As is often the case, Internet technology and its social utility have surpassed the development of the law and prevent law enforcement from carrying out its mandate to investigate such matters. Posted child abuse imagery is analogous to a physical poster or TV advertisement showing real child abuse. The community would agree that such a practice would be abhorrent and offensive to the community standards of tolerance. However, this conduct is currently permitted online despite the Internet's reach being must greater than any advertisement or physical poster. Notably, as the Internet displays content globally and at the leisure of any user, any time of day with anonymity, it results in the continued and ongoing re-victimization of the child causing further trauma and harm.

To remedy the public Internet posting of child physical abuse imagery the law must prohibit the conduct and provide the commensurate methods of investigation and removal. This can be facilitated through amending the *Criminal Code* to create a new section to prohibit Internet posting or deem child abuse imagery as obscene while amending the existing removal provisions to include child abuse imagery.

Resolution #03 - 2016

REASONABLE LAW TO ADDRESS THE IMPACT OF ENCRYPTED AND PASSWORD-PROTECTED ELECTRONIC DEVICES

Submitted by the Law Amendments Committee

WHEREAS electronic devices are ubiquitous in both the licit and illicit facets of modern society, and;

WHEREAS electronic devices can be and are used to facilitate the commission of serious and multi-jurisdictional crime, such as organized crime, violent crime, fraud and other financially-motivated crime, and Internet and computer-related crime, and;

WHEREAS Internet and computer-related crime is a growing area of criminal activity that threatens Canadians' privacy and security interests, and Canada's financial systems, and;

WHEREAS the contents of electronic devices can yield critical evidence of such crimes, and;

WHEREAS users of electronic devices have ready access to encryption and password-protection that renders the contents inaccessible to public safety agencies and, not withstanding a valid judicial authorization to search those contents, and;

WHEREAS the inability to execute judicially authorized searches of electronic devices has and will bring serious criminal, and national security investigations to abrupt and unsuccessful ends, and;

WHEREAS there is no legislative power specifically designed to compel an individual to provide either law enforcement or public safety agencies with the password or encryption key for an electronic device, the search of which has been judicially authorized;

WHEREAS other jurisdictions have afforded law enforcement agencies with such legislative powers, and have achieved success in defending that legislation and in furthering legitimate law enforcement interests, and;

WHEREAS this is a possible solution being requested, and;

WHEREAS the Canadian Association of Chiefs of Police, as the national voice of Canadian police leadership, is committed to raising issues where the Criminal Code should be amended.

THEREFORE BE IT RESOLVED that the Canadian Association of Chiefs of Police urges the Government of Canada, for the purpose of community safety, to identify a legislative means for public safety agencies inclusive of law enforcement, through judicial authorization, to compel the holder of an encryption key or password to reveal it to law enforcement.

Resolution #03 - 2016

REASONABLE LAW TO ADDRESS THE IMPACT OF ENCRYPTED AND PASS-WORD PROTECTED ELECTRONIC DEVICES

Background

James B. Comey, Director of the Federal Bureau of Investigation, described the U.S. experience with encrypted and password-protected electronic devices as follows: "Armed with lawful authority, we increasingly find ourselves simply unable to do that which the courts have authorized us to do, and that is to collect information being transmitted by terrorists, by criminals, by pedophiles, by bad people of all sorts." In response, the National District Attorneys Association and the International Association of Chiefs of Police are supporting legislation, a discussion draft of which was released on April 13, 2016, that would compel companies to provide "technical assistance" to law enforcement in respect of encrypted and password-protected data.

Canadian law enforcement faces the same investigative challenges and requires an analogous legislative response. However, legislation directed at companies, many of which will be located outside of Canada, may not suffice. Law enforcement requires reasonable, constitutionally-compliant legislation crafted to suit the Canadian context.

Digital security technology has now advanced to the point that impenetrable password protection and encryption are readily – and in many cases *freely* – available on all electronic devices. This technology immunizes legally seized electronic devices from the execution of a judicially-authorized search, and often compels the abrupt and unsuccessful end of a serious criminal investigation. Recent law enforcement experience provides specific examples of criminal investigations that have been derailed in this manner.

While the issue potentially bears on a wide range of investigations, it will have particular ramifications for the investigation of online child sexual exploitation and abuse, fraud and other financially-motivated crimes, organized crime, requests for international law enforcement assistance, and national security matters involving suspected extremism and other threats to Canada.

Furthermore, technical advancements in techniques to crack password-protected devices alone will not suffice in the case of newer devices with operating systems that erase data (wiping clean) after a limited number of unsuccessful password attempts.

While there are numerous benefits that encryption provides to assure privacy and to cyber security such as e-commerce, it is contrary to the public interest to permit criminals or those that threaten the security of Canadians to create a zone of immunity by encrypting and password-protecting their data, and to thereby limit the reach of validly-issued judicial authorizations. In contrast, a reasonable and proportional law that would permit law enforcement to access encrypted and password-protected data, in appropriate cases, through the application for and granting of a judicial authorization, would promote the safety of Canadian children on the

Internet, enhance the integrity of Canadian financial system, improve national security, and assist in the investigation and prosecution of organized and violent criminals. It must be emphasized that Canadian law enforcement agencies have identified this public safety gap and are seeking a legislated process where a judicially authorized format may compel the production of a password or encryption key. It is recognized the use of this privacy-intrusive legislated framework would need to be balanced on a concept of proportionality.

In January 2015, in his address to the Annual Symposium of the Canadian Association for Security and Intelligence Studies, when describing challenges of the basic problem for law enforcement to acquire information, RCMP Commissioner Paulson stated: "We also, and perhaps more urgently, need new tools, to be able to enforce the criminal law quickly and efficiently, in a way consistent with Canadian values and the Charter of Rights and Freedoms".

Recent Law Enforcement Experiences

Several recent examples from the United States and Canada highlight the gravity of this problem:

- In 2010-2011, the Ontario Provincial Police investigated a male for setting up hidden cameras in his house to spy on a young woman who worked for his wife. Police obtained a warrant to search the house and found an encrypted hard drive hidden in the rafters of the basement. E-Crimes could not break the encryption. Police ultimately discovered documents and books containing the suspect's computer information, and entered a series of possible passwords until one of them opened the hard drive. Thousands of voyeuristic images were obtained from the device. The investigating officer explained that the investigation would have failed if the suspect had not written down the password in those documents.

- In 2012, police lawfully seized computers from Justin Gryba in Saskatoon in relation to a child pornography investigation. Some of the computers had been locked and encrypted. Mr. Gryba refused to provide the passwords. Forensic technicians from Saskatoon and Ottawa were not able to break the encryption on one device until two-and-a-half years later. That device contained child pornography depicting many different victims. Mr. Gryba was charged with making and possessing child pornography and, on April 15, 2016, sentenced to serve a further two years less a day in custody (on top of 29 months' credit).

- In May 2013, the Ontario Provincial Police received information that an individual had child pornography on his Apple iPad and potentially on his Apple Macbook Pro laptop. A warrant was executed at the individual's residence and the devices were seized. The items were submitted to OPP E-Crimes for examination and retrieval of any images. Both items were password-protected. E-Crimes did not have the capabilities to gain access without the password. The investigating officer was unable to obtain Production and Assistance Orders for Apple in California, and would have been unwilling to send the devices to California given their probable illegal content. The officer also could not obtain a destruction order, and was forced to make arrangements to return the devices to the suspect. Conditions of return were negotiated: the suspect would provide the

password for the purpose of wiping the devices before their return, and no charges would be laid.

- Between October 2014 and June 2015, law enforcement in Manhattan, New York, seized 74 Apple iPhones related to investigations into offences such as the attempted murder of three individuals, the repeated sexual abuse of a child, an ongoing sex trafficking ring, and numerous assaults and robberies. Warrants to search the devices were obtained, but could not be executed.

- In Fort Frances, Ontario, there was a recent case of theft of narcotics from a hospital. A phone was seized and forwarded to the Ontario Provincial Police Technological Crime Unit ("E-Crimes"), which was unable to unlock it. The investigation has stalled, though OPP E-Crimes suggested they "might" be able to use a new software program to unlock the phone in 8-12 months.

- In June 2015, a father of six was shot dead in Evanston, Illinois, 10 miles north of Chicago. There were neither witnesses nor surveillance footage. Investigators found an Apple iPhone and a Samsung phone running on Google's Android operating system next to the body of the deceased. Both devices were password-protected. An Illinois state judge issued a warrant ordering Apple and Google to unlock the phones and share with authorities any data that could potentially solve the murder. Apple and Google replied that they could not do so without knowing the user's passcode. The murder remains unsolved.

Potential solutions: other jurisdictions' experiences

Canadian law enforcement may have the ability to compel the production of biometrics through an impression warrant (s. 487.092) or a general warrant (s. 487.01), but not the production of passwords or encryption keys. Several other jurisdictions have explored or implemented legislation to the permit the latter:

- The United Kingdom's *Regulation of Investigatory Powers Act 2000* empowers the court to order a person to supply decrypted information and/or encryption keys. The legislation has been unsuccessfully challenged on self-incrimination grounds.

- Australia's *Cybercrime Act 2001* provides authorization for a magistrate to order a specified person, including a suspect or an accused person, to provide any information or assistance that is reasonable and necessary to allow law enforcement to access, copy, and convert electronic data, with a penalty for non-compliance.

- Key production legislation is in force in South Africa (*Regulation of Interception of Communications and Provision of Communication-Related Information Act*), France (*Loi sur la sécurité quotidienne*), and Finland (*The Coercive Measures Act (Pakkokeinolaki)).*

- Sweden has recently proposed encryption key production legislation.

- New Zealand Customs released a Discussion Paper in 2015 proposing new powers in the *Customs and Excise Act* to demand passwords from persons crossing the border.

- The United States has yet to fully embrace key production, but there have been instances of judges subpoenaing accused individuals to provide their passwords to law enforcement. U.S. Courts have yet to fully resolve whether compelled key production or compelled production of an unencrypted copy of encrypted data violates the privilege against self-incrimination protected by the Constitution's Fifth Amendment.

  However, on April 13, 2016, U.S. Senate Intelligence Committee Chairman Richard Burr and Senator Dianne Feinstein, released a discussion draft of proposed legislation ("Compliance with Court Orders Act of 2016") that would address encrypted and password-protected electronic devices by directing the relevant company to decrypt data or provide other technical assistance to law enforcement. Their proposal is supported by the National District Attorneys Association and the International Association of Chiefs of Police.

Further review of the legislation in the United Kingdom:

The legislation in the United Kingdom was further examined because of its well-established encryption key/password production legislation and our shared legal and constitutional principles. A summary of data from the Office of Surveillance Commissioners ("OSC") Annual Reports provided further insight about the efficacy of that legislation. The OSC is a public body sponsored by the Home Office that oversees the conduct of covert surveillance and covert human intelligence sources by public authorities in accordance with the Regulation of Investigatory Powers Act 2000 ("RIPA").

Section 49 of the RIPA, activated by ministerial order in October 2007, requires persons to supply decrypted information and/or encryption keys to state representatives upon receipt of a court order. In practice, an application involves the following steps:

- The Home Office National Technical Assistance Centre ("NTAC") must approve the application for the service of an s. 49 notice.
- Once NTAC approval is in place, permission may be sought from a Judge.
- Once judicial permission is given, the s. 49 notice should be served.
- If a person fails to comply with the s. 49 notice, a criminal charge may be laid.

The OSC has reported annually on the use of s. 49 since its 2008-2009 Annual Report. The most recent Report is for 2014-2015. The available data from 2008 – 2015 suggests the following:

- 160 notices were issued under s. 49 of *Regulation of Investigatory Powers Act:*

    - The investigations consistently involve terrorism, domestic extremism, indecent images of children, insider dealing, fraud, evasion of excise duty and drugs.

    - Investigations into human trafficking and kidnapping of children seem to be an emerging issue.

- Between 38 and 42 individuals (~24% to ~26%) complied with the notice;[7]
- 93 individuals (~58%) did not to comply with the notice;[8]
- 68 of those individuals were charged;
- 46 of those individuals were prosecuted; and
- 14 prosecutions resulted in convictions.

[7] The 2008-2009 Report does not set out the number of notices complied with or still pending. Since the Report provides that 15 notices were issued and that 11 notices were not complied with, this estimate was generated using the minimum (0) and maximum (4) number of individuals who could have complied.

[8] This percentage does not account for notices that are still pending. Year-to-year percentages for non-compliance have questionable explanatory value, given the overlap in data across reporting years. To the extent that they are useful as a benchmark, they are as follows:

- 2008-2009 (~73%);
- 2009-2010 (~41%);
- 2010-2011 (~17%);
- 2011-2012 (~75%);
- 2012-2013 (~73%);
- 2013-2014 (~52%);
- 2014-2015 (~59%).

Resolution #04 - 2016

INCREASE MEASURES TO FURTHER RESTRICT THE AVAILABILITY AND USE OF REACTIVE TARGETS IN CANADA

Submitted by the Law Amendments Committee

WHEREAS reactive targets, commonly referred to as exploding targets, are specifically designed to be detonated by standard or high velocity rifle fire and used for long-range target practice, and;

WHEREAS reactive targets are a binary explosive sold in multi-ingredient kits in Canada. When the components of these binary kits are mixed together, a high explosion is produced. More precisely, reactive targets have a power output, expressed as TNT equivalency[9], of approximately 0.82, and;

WHEREAS reactive targets are regulated under the *Explosives Regulations, 2013* and are authorized to be sold online and through retail establishments to individuals possessing a valid Firearms Possession and Acquisition License (PAL) or a Fireworks Operator Certificate, and;

WHEREAS an individual can purchase, transport and store up to 20 kilograms of reactive targets at a time under the current regulatory framework without any additional permits or licences, and;

WHEREAS despite being intended for long-range target practice, the Internet and social media contain a plethora of examples demonstrating the misuse of reactive targets in Canada and abroad, and;

WHEREAS police in Canada have investigated several cases of misuse or criminal use of reactive targets including cases involving improvised explosive devices (IEDs), and;

WHEREAS research and testing by Canadian police and security partners have demonstrated that reactive targets can be easily weaponized and incorporated into powerful and destructive IEDs for criminal and terrorist purposes, and;

WHEREAS reactive targets pose a direct threat to public safety and first responders by taking the guesswork out of homemade explosives manufacturing.

THEREFORE BE IT RESOLVED that the Canadian Association of Chiefs of Police urges the federal, provincial and territorial governments to prevent the misuse and criminal and terrorist use of reactive targets by increasing measures to further restrict their availability and use in Canada.

[9] TNT equivalent is a convention for expressing the energy released in an explosion.

Resolution #04 - 2016

INCREASE MEASURES TO FURTHER RESTRICT THE AVAILABILITY AND USE OF REACTIVE TARGETS IN CANADA

Background

Reactive targets, commonly referred to as exploding targets, are specifically designed to be detonated by standard or high velocity rifle fire and used for long-range target practice. In other words, reactive targets are meant to explode when hit by the round of a rifle during long-range target shooting; making it easier for the shooter to confirm that the intended target was accurately hit.

Reactive targets are a binary explosive sold in multi-ingredient kits under several brand names in Canada including Tannerite, Thundershot, Sure Shot, KaBoom and Shockwave. A binary explosive is an explosive consisting of two components, neither of which is explosive by itself. In the case of reactive targets, the two components are ammonium nitrate or an ammonium nitrate / potassium perchlorate mixture (Part A) and an aluminum or magnalium alloy powder (Part B). When Parts A & B are mixed together, a high explosive is produced. More precisely, reactive targets have a power output, expressed as TNT equivalency, of approximately 0.82.

In Canada, the acquisition, transport, storage and use of reactive targets is regulated under the *Explosives Regulations, 2013*. In October 2014, the Explosives Safety and Security Branch of Natural Resources Canada (NRCan) published guidelines respecting the sale of reactive targets.[10] Individuals possessing a valid Firearms Possession and Acquisition License (PAL) or a Fireworks Operator Certificate (FOC) can purchase, transport, store and use up to 20 kilograms of reactive targets. Quantities in excess of 20 kilograms can be purchased and stored by acquiring a magazine licence from NRCan for an annual fee of $70.00.

Despite being designed for long-range target shooting, there is ample evidence available on the Internet and through social media sites demonstrating the misuse of reactive targets in Canada and abroad. Although contrary to manufacturing instructions and/or regulatory guidelines, multiple reactive targets are being combined to produce very powerful explosions capable of completing destroying buildings and automobiles and severely injuring people and wildlife. Publically available videos from Canada and the U.S. demonstrate the destructive nature of reactive targets when misused.

- Echoes of gunfire and exploding targets trigger residents' fears (Canada) – http://globalnews.ca/video/2655114/echoes-of-gunfire-and-exploding-targets-trigger-residents-fears

[10] http://www.nrcan.gc.ca/explosives/publications/guidelines/16729

- 4 pounds of Thundershot exploding targets (Canada) – https://www.youtube.com/watch?v=_hZRbLBn2K8

- 164lbs of Tannerite Kills a Barn (U.S.) – https://www.youtube.com/watch?v=edRbcTXAijY

- 250lb. EXPLODING TARGET (U.S.) – https://www.youtube.com/watch?v=osrWmQtyatw

- Blowing Up A Car With 50lbs. of Tannerite (U.S.) – https://www.youtube.com/watch?v=7DK_pw2tq2Q

- 40lbs tannerite vs. Jetta (U.S.) – https://www.youtube.com/watch?v=-oyoY_5Vp64

In response to wildfire and public safety concerns, the U.S Forest Service prohibited the use of reactive targets on national forest lands. Over a two year period (2012-14) reactive targets were linked to several wildfires in U.S. national forests which cost some $30M to supress.[11]

Reactive targets have been a source of concern for U.S. law enforcement agencies. In March 2013, the FBI issued an intelligence bulletin given concerns over the potential illicit use of reactive targets by criminals and extremists.[12] Furthermore, U.S. law enforcement agencies have discovered the use of reactive targets in improvised claymore mines, pipe bombs and other IEDs.

In addition to media reports of misuse[13][14], Canadian law enforcement agencies have also encountered instances of misuse and criminal use of reactive targets:

- **April 2016:** a traffic stop and subsequent search of a residence resulted in the seizure of two IEDs and the discovery of reactive target mixtures.[15]
- **Since 2014:** criminal use of reactive targets has been linked to four RCMP investigations involving the destruction of property through post-blast residues.[16]
- **May 2012**: RCMP charged two persons who shot six pounds of reactive targets in a washing machine. The resulting fire caused $30K in property damage and cost $60K to extinguish.[17]

[11] http://gazette.com/u.s.-forest-service-to-ban-exploding-targets-in-colorado/article/1504412
[12] https://publicintelligence.net/fbi-exploding-targets/
[13] http://www.cbc.ca/news/canada/manitoba/neighbours-tackle-trash-at-seddons-corner-cleanup-1.3100513
[14] http://globalnews.ca/news/2655045/litter-vandalism-in-ghost-valley-are-growing-concern/
[15] http://www.cbc.ca/news/canada/edmonton/speeding-driver-in-edmonton-caught-with-drugs-guns-and-explosives-1.3552490
[16] http://www.wltribune.com/news/284005611.html?mobile=true

[17] http://www.comoxvalleyrecord.com/news/160620805.html?mobile=true

Importantly, research and testing by Canadian police and security partners have demonstrated that reactive targets can be easily weaponized and incorporated into powerful and destructive IEDs for criminal and terrorist purposes.

Notwithstanding Canada's regulatory framework, the Canadian Association of Chiefs of Police believes that reactive targets pose a direct threat to public safety and first responders by taking the guesswork out of homemade explosives manufacturing. Given these concerns, the Canadian Association of Chiefs of Police urges the federal, provincial and territorial governments to prevent the misuse and criminal and terrorist use of reactive targets by increasing measures to further restrict their availability and use in Canada.