CYBERBULLYING

Training for
Justice System Personnel

2nd Edition

SAFER SCHOOLS TOGETHER

Acknowledgements:

Safer Schools Together is dedicated to educating professionals on the importance of understanding, preventing and providing effective intervention as they relate to the issues of bullying, cyberbullying and threatening behaviours. We would like to acknowledge the Department of Justice Canada and Youth Justice, Ministry of Children and Family Development for making this project possible.

During the development of this training, numerous consultations took place with educators, the Criminal Justice Branch, Victim Services, restorative justice professionals, police officers (RCMP and municipal forces), and Youth Justice. Safer Schools Together appreciates the thoughtful contributions provided by individuals and agencies whose experience, knowledge, dedication and insight continually inspire our dedication to ensure safe and caring communities. These include many professionals across Canada who participated in consultative groups, made valuable contributions to the development and implementation of the training, and provided insightful feedback throughout the development of this training resource.

The Project Advisory Group
Anne Kimmitt, Youth Justice Consultant, Youth Justice Program Support, Ministry of Children and Family Development
Phil Peachey, Youth Probation Supervisor, Ministry of Children and Family Development
Jim Hughes, Chief Legal Technology Counsel, Criminal Justice Branch
Linda Selbie-MacDonald, Administrative Crown Counsel, Vancouver Youth Court, Criminal Justice Branch
Lynett Jung, Professional Development Coordinator, Criminal Justice Branch
Dina Green, Deputy Provincial Director, Corrections Branch
John Cordeiro, Program and Policy Analyst, Corrections Branch
S/Sgt T.E. (Tom) Norton, Ops NCO, Crime Prevention Services, RCMP BC "E" Division
Vijay Morancie, Crime Prevention Services, RCMP BC “E” Division
Erin Hobday, Victim Services and Crime Prevention Division
Randeep Tut, Project Manager, Safe Schools, Ministry of Education

Professionals
J. Kevin Cameron, Executive Director, Canadian Centre for Threat Assessment & Trauma Response
Heather Hildred, Victim Services Program Director, RCMP BC “E” Division
Catherine Bargen, Restorative Justice Coordinator, Ministry of the Solicitor General
Daniel M Scanlan, Crown Counsel, Crown Law Division, Ministry of Justice
R. Kyle Friesen, Counsel, RCMP Legal Advisory Section
Cpl. Rafael Alvarez, Provincial Youth Strategies RCMP
Tanya Whysker, Detective Constable, Vancouver Police Department
Clint Baker, S/Sgt. NCO i/c Vancouver Integrated Technological Crime Unit RCMP
Monique St. Germain, General Counsel, Canadian Centre for Child Protection
Noni Classen, Director of Education, Canadian Centre for Child Protection
Kim Leifso, SPERAS Counsulting

Contributing Authors
Koryna Kirkpatrick, Sam Jingfors, Linda Selbie-MacDonald, Erin Hobday, Anne Kimmitt, Phil Peachey and Theresa Campbell.

Introduction:

Youth today are online, mobile and connected more than ever before. Their heads are down and their eyes lit up by their digital device. Their sense of self-esteem, self-worth and identity appears to be validated through "likes" and feedback on their posts as they disclose their lives to an audience of peers, acquaintances and others. Technology is a part of our everyday life and provides many new and positive educational benefits but also increases our concerns around issues that affect personal safety and identity. Before technology, children and youth were safe from those who bullied them once they were at home. Today digital devices facilitate and perpetuate bullying behaviours. These devices allow youth to access social networking sites anytime they wish and send images and video messages to anyone with a device. Technology is a true gift for individuals who engage in these behaviours. They don't have to look at their victims and they don't have to deal with immediate, negative reactions from bystanders.

There is a clear generational gap in understanding communications technology today. The implication of this gap is that those who are expected to take action may lack the understanding of technology, the knowledge to relate to the issues, and the means to respond effectively.

When discussing cyberbullying behaviour, we must note the importance of the language that is used to describe the outcome. The terms "target" and "victims" will be used interchangeably for the purposes of this this training. In many cases, cyberbullying behaviour can be in response to something that has happened in the past and may be retaliatory vs. offensive in nature. Investigating everyone's role in a reported incident is paramount in responding effectively.

In consideration of the *Youth Criminal Justice Act*, there is a motivation to consider and divert youth cases whenever possible to avoid criminalization of adolescent behaviour. However, there are concerns that taking these measures may not always be enough to hold a young person accountable. Education and understanding of the YCJA and its available options, including restorative processes, must be provided to ensure appropriate outcomes based on the individual merits of each situation.

There needs to be room for dialogue as we engage in educating others on the impact of cyberbullying. When referring to the unsettling trends of suicide amongst young people, we need to find an appropriate response to the behaviour in those cases where youth are not only encouraging, but also supporting other users/peers in their expression of suicidal ideation/completion and sometimes offering an improved plan for completion. There is a concerning increase in these types of behaviours with the escalating presence of anonymous websites and social networking applications such as Ask.fm, Yik Yak and Whisper.

This is troubling for professionals as Counseling Suicide, under the Criminal Code, was a law created to address the notion of assisted suicides. It is deemed an indictable offence and thereby the punishment is more serious. As a result, we are not aware of any Canadian cases where a young person has been charged with counseling suicide. However, the fact that this offence is indictable should not affect whether youth are charged. It is important to note that youth are routinely charged with offences that are solely indictable (e.g. robbery, break & enter).

When supporting both those who have engaged in, and/or been targeted by cyberbullying, we must ensure that we are providing relevant education, effective modelling and coping strategies for all parties.

Table of Contents

Bullying

The word bullying in today's landscape has grown into an umbrella term used to describe a wide variety of inappropriate, hurtful, violent, and negative youth behaviours. For the purposes of this training, a more concise definition is needed. Bullying behaviour involves the systematic abuse of power through unjustified and repeated acts intended to hurt or inflict some form of harm. Its impact can be direct (physical and verbal teasing) or indirect (relational, such as social exclusion and spreading nasty rumours).[1]

Bullying is any pattern of persistent unwelcome or aggressive behaviour intended to make others uncomfortable, scared or hurt. It is used as a means of control. Bullies get a sense of power from taking advantage of and disparaging those they may target based on appearance, culture, race, religion, ethnicity, sexual orientation or gender identity.

School staff, police officers and parents alike must be vigilant and be aware that some bullying behaviours breach the Canadian Criminal Code and law enforcement needs to be involved.

Bullying can generally be divided into four different categories:

- **Physical Bullying:** may include tripping, pinching and pushing or damaging property.
- **Verbal Bullying:** may include name-calling, insults, teasing, intimidation, homophobic or racist remarks or verbal abuse.
- **Social, Emotional and Relational Bullying:** use of behaviours instead of fists to deeply hurt others, is often harder to recognize and can be carried out behind the target's back. It is designed to harm a person's social reputation and/or cause humiliation. Social, emotional and relational bullying includes:
    - Lying and spreading rumours.
    - Negative facial or physical gestures, menacing or contemptuous looks.
    - Playing nasty jokes to embarrass and humiliate.
    - Mimicking unkindly.
    - Encouraging others to socially exclude someone.
    - Damaging someone's social reputation or social acceptance.
    - Segregation and exclusion from any kind of social activity

Relational bullying is a type of bullying behaviour that can include physical aggression, taunting, harming others through damaging their peer relationships and social isolation. Boys can exhibit this behaviour but relational bullying is more often seen in girls. In a recent study released by MediaSmarts, it was interesting to note that the results of their survey showed that males tended to

[1] CCSO Cybercrime Working Group - Report to the Federal/Provincial/Territorial Ministers Responsible for Justice and Public Safety - Cyber bullying and the Non-Consensual Distribution of Intimate Images - Department of Justice Canada - June 2013

harass via online gaming and had a higher tendency to make negative comments regarding race, religion, ethnicity or sexual orientation, while females were more likely to forward photos to make fun of others and name call. [2]

Relational bullying behaviour is learned at an early age and is generally seen in children who feel lonely and depressed. It is not linked with socioeconomic status.

Targets of relational bullying and aggression are socially and emotionally at risk, due to constant harassment. The harassment can be direct and involve intimidation in front of peers; or it can be indirect and involve intimidation through social media sites and email. Either way, it is constant.

Youth who are the frequent targets of relational bullying can feel rejected, depressed and submissive; and often see no resolution of the situation.

Cyberbullying

Cyberbullying behaviour involves the one time or repeated use of electronic information and communication technologies to engage in conduct or behaviour that is intended, or ought reasonably to be expected to cause fear, intimidation, humiliation, distress or other damage or harm to another person's health, emotional well-being, or reputation. This may also include online posting or electronic distribution of embarrassing pictures/intimate images or videos, real or altered, without the consent of the person contained in the images. Cyberbullying is overt or covert bullying behaviour using digital technologies. Other examples include harassment via digital devices, setting up defamatory personal websites or deliberately excluding someone from social networking spaces. Cyberbullying can happen at any time. It can be in public or in private and sometimes is only known to the target and to the person perpetuating the bullying behaviour.

Cyberbullying is the newest phenomena of the four types of bullying. Given the pace of the development of new technology and the younger age at which young people are introduced to digital devices and the Internet, information and trends on this type of bullying behaviour changes rapidly. Often digital technologies will be combined with social, emotional and relational bullying to socially assassinate the character of a youth and to isolate him/her from peers.

Social Assassination

Online attacks are increasingly clever and creative. The simple way to define this behaviour would be to call it what it is: social assassination. The term may seem aggressive, but so is the behaviour. We need to identify this behaviour for what it really is and look at ways of stopping the victimization occurring across North America as a result (Campbell, 2009).

Youth continually find new online sites and communities to attack the character and reputation of others.

[2] Young Canadians in a Wired World, Phase III: Cyberbullying: Dealing with Online Meanness, Cruelty and Threats, MediaSmarts, 2014.

Social assassination behaviours include but are not limited to: websites targeting youth through humiliation, humiliating others while playing online games, inflammatory and derogatory posts on Discussion Boards, Hate Contracts, Newsgroups, or Guest Books. Social assassination can also include postings on social networking sites or personal polling websites that encourage students to vote. For example, pictures of students are being posted and rated in public forums.

It has become evident that posting comments to various types of social media sites is very simple. However, removing these derogatory and hurtful posts can be a challenge. Many of these websites are hosted in different countries governed by different laws, are difficult to make contact with, and are often unwilling to remove any content from their website, stating that their site is a venue for individuals to post and exchange opinions.

Cyberbullying has changed the traditional face of bullying in three significant ways – Access, Scope, and Anonymity (ASA).

- **Access:** It is virtually impossible for targets to get away from those who cyberbully. Most youth have access to all types of technology, which provides those who cyberbully the ability to reach their targets almost all the time. Targets do not have a safe haven as they do in cases of traditional bullying.

- **Scope:** Unlike traditional bullying, due to technology, audiences of cyberbullying have few barriers and can grow exponentially.

- **Anonymity**: Cyberbullying is not a face-to-face interaction and those who cyberbully have the ability to hide behind technology. Anonymity, which is inherent in electronic communication, promotes a lack of inhibition. As a result, normal behaviour restraints can disappear, allowing youth to act harsher than they would offline.

Impact of Cyber Bullying Behaviour: What makes this Different?

Although each individual is unique when it comes to responding to bullying, there are some specific factors that make targets/victims of cyberbullying different from targets/victims in other types of bullying and/or criminal cases. These include:

- 24/7 availability of the Internet;
- Possible anonymity of the perpetrator
- Scope of audience and permanence of the victimization

24/7 Availability of the Internet

Unlike conventional, face-to-face bullying, there is no escape from the torment that can be caused by the negative online comments, repeated messaging and taunts that can occur with cyberbullying. Cyberbullying can happen anywhere, at any time, and even in places where a victim may traditionally feel safe, like their home.

To prevent the behaviour, the onus can fall to victims to "shut down" their devices and avoid further contact with those who may be harassing them online. Although, it would be ideal if victims could simply do this, we know that this not easy thing for young people. For many youth, having an online presence is an essential part of their social interaction and connection. Shutting down their devices could mean that they are losing that connection, and also potentially losing the positive support that they could receive from their online network.

It is also important to remember that even if a victim is not "plugged in" or reading the comments online, other people are, and it won't help the situation improve or go away for the victim.

Possible Anonymity of the Perpetrator

One of the biggest issues in tackling cyberbullying are the applications (apps) that allow perpetrators to be anonymous, Anonymity has the potential to cause increased fear for the victim as they cannot pinpoint WHO is actually attacking them online. Anonymity does not make it easier for victims. Falling prey to this type of behaviour erodes self-esteem and self-confidence in even the strongest young person. Moreover, the anonymity of being online can make the perpetrator actually take the level of harassment further, because they are unable to see the victim's reaction. When we consider the extreme importance of social acceptance in the lives of a young person, it becomes very clear how severe the impact of victimization can be.

Scope of Audience and Permanence of the Victimization

Young people typically understand the impact of being exposed and humiliated online. They know that one posted message can be forwarded on to thousands of people in mere minutes. They know that regardless of posts being removed, the effect will feel permanent for them. It will always be out there somewhere. When we consider the scope of the information shared, and the sheer volume of people who may be aware of their situation, it can lead to very intense feelings of humiliation. This intensity can lead towards a negative self-image, self-harm, depression and isolation from everyone who knows about the incident (school, staff, parents, friends, etc.)

Trends regarding Victimization and the Correlation to Self-Harm and Suicidal Ideation/ Completion

More adolescents are accessing emergency rooms across Canada with self-inflicted wounds, or after suicide attempts, than we have ever seen before. We need to understand the correlation between this identified increase and cyberbullying behaviours (social assassination). Commonly it is kids aged 12 to 17 who are "cutting;" slashing their arms, thighs or bellies with everything from razor blades, pencils to the sharp edges of protractors.

It can be doing anything to physically hurt themselves. We are seeing kids burning themselves, bruising themselves by repeatedly banging their fist or other parts of their bodies against the walls, doors and other hard instruments. It's a way for them to focus on another form of pain. Dr. Hazen Gandy, MD, FRCPC, Head of Child and Adolescent Psychiatry Division, Department of Psychiatry, Faculty of Medicine, University of Ottawa noted that "self-harming is a symptom of deeper issues such as anxiety or depression that stem from complex causes." It is becoming clear how climbing caseloads in mental health are affecting the health system.

Doctors say they are not only seeing a distressing rise in the number of kids seeking help for self-inflicted wounds, but many specialists report that they don't have the hallmarks of a psychiatric disorder. That is leaving doctors with no clear answers as to why they're seeing so many more kids with these kinds of injuries.[3]

More and more kids are also posting their self-harm behaviours online, including still images and videos of them cutting. The majority of the people that are visiting these sites are "liking" the posts or requesting more. This is quite alarming and we should be very concerned as a society. While this behavior continues we can predict that the number of young people/adolescents engaged in these behaviours will continue to rise. We could refer to this as contagion effect.

Self-harming behaviours and suicide attempts are very different behaviours and need to be responded to accordingly. When we become aware that a young person who is contemplating suicide has posted their thoughts online we must have the hypothesis that their justification to complete the suicide is higher than those who do not post online. All of these behaviours are cries for help and should be responded to. However, the trend is that when kids talk about killing themselves online, most respondents to their posts like the post, or tell them to hurry up and do it; potentially escalating their level of commitment to complete the act.

As educators and advocates we, at SST, are very concerned of the contagion effect through social media but also news media. There continues to be cyberbullying prevention ads and educational messaging inferring that cyberbullying is the cause of suicides. This is not the case. We agree that it is a risk enhancer for anyone already dealing with a level of emotional pain and provides further justification for someone already on the pathway of considering suicide.

In the Victim Services Guidelines more will be discussed on this topic specifically regarding self-harm and suicide. Understanding the behaviour is key to responding and supporting young people appropriately. Please refer to page 58.

[3] Alison Auld and Sue Bailey, CP (2014, March 15). More teens showing up at ERs. http://www.cbc.ca/news/canada/canadian-hospitals-stretched-as-self-harming-teens-seek-help-1.2574316

Current Trends of Youth Behaviour Online

As of early 2015 the worldwide population grew to over 7.2 Billion people, 3.01 Billion of which are active Internet users and over 2.078 have active social media accounts (We are Social, 2015). Canadian youth today are no exception and are more online, mobile and better connected than ever before. Their heads are down and their eyes lit up by the screen of their smartphone, they connect and socialize with their peers through social media and text their parents from upstairs in their own home. Self-esteem is validated through likes and feedback on their posts as they self-disclose their lives to a stadium audience of peers and others. Their devices have become their portable and personal lifeline portals to online access and without them, they can feel lost. The current statistics indicate just how attached our youth are to the wireless world:

- Mobile devices and smartphones are the main access points of young people connecting to the internet
- Internet access is universal, with 99% of students able to access the Internet outside of school.
- Close to half (49%) of students in Grade 4 have access to their own phone or someone else's phone regularly.
- Almost one-third of students in Grades 4-6 have a Facebook account, in spite of its terms of use agreement that bars children under the age of 13 from using the site.
- 82% of youth were online/on their phone after they were supposed to be asleep.
- Nearly 50% of youth under 15 reported having been cyberbullied in the last month
- 41% of youth under 15 said they wouldn't report online abusive content because they think the person reporting would find out

2015 PEW Research Center Data reports that:

- 92% of teens report going online daily, and 24% say they go online "almost constantly"
- Facebook remains the most used social media site, with 71% of teens using it, Instagram follows behind at 52%, Snapchat (41%), and Twitter (33%)

Sources: *Mediasmarts [2014] Young Canadians in a Wired World: Life Online, 2014 McCreary Center BC Adolescent Health Survey; PEW Research Center: Teens, Social Media & Technology Overview 2015; PREVNet Social Media and Safety Survey [2014]; We Are Social: Digtial, Social & Mobile Worldwide in 2015*

Cyberbullying and the Canadian Criminal Code

As the law currently stands, there is no specific or stand-alone crime of cyberbullying. However, when the bullying behaviour reaches the level of criminal conduct, the current Criminal Code contains several offences that capture this criminal behaviour. The following Criminal Code offences may apply to the behaviours associated with cyber bullying:

- Criminal Harassment (s.264)
- Uttering Threats (s.264.1)
- Child Pornography - Making of, Distribution, Production, and Accessing (s.163.1)
- Luring a Child (s.172.1)
- Voyeurism (s.162)
- Publication, etc., of an intimate image without consent (s.162.1)**
- Intimidation (s.423(1))
- Mischief in Relation to Data (s.430 (1.1))
- Unauthorized Use of Computer (s.342.1)
- Identity Fraud (s.403)
- Extortion (s.346)
- False Messages, Indecent or Harassing Telephone Calls (s. 372(1))
- Counselling Suicide (s.241)
- Defamatory Libel (s.298-302)
- Incitement of Hatred (s.319)

** s.162.1 of the Criminal Code was amended to address the non-consensual distribution of intimate images due to the increase in sexting related incidents nationwide. This change was included in the recent Anti-Cyberbullying legislation called the *Protecting Canadians from Online Crime Act* (Bill C-13), which came into effect on March 9th, 2015

From a review of the case law, the following offences are most commonly charged in response to cyberbullying:

- **Criminal Harassment (Section 264) [Hybrid Offence]**
  - 264. (1) No person shall, without lawful authority and knowing that another person is harassed or recklessly as to whether the other person is harassed, engage in conduct referred to in subsection (2) that causes that other person reasonably, in all the circumstances, **to fear for their safety or the safety of anyone known to them**.

- **Prohibited Conduct**
  - (2) The conduct mentioned in subsection (1) consists of:
    (a) repeatedly following from place to place the other person or anyone known to them;

b) repeatedly communicating with, either directly or indirectly, the other person or anyone known to them;
(c) besetting or watching the dwelling-house, or place where the other person, or anyone known to them, resides, works, carries on business or happens to be; or
(d) engaging in threatening conduct directed at the other person or any member of their family.

- **Uttering Threats (Section 264.1) [Hybrid Offence]**
  - 264.1 (1) Every one commits an offence who, in any manner, **knowingly utters, conveys or causes any person to receive a threat**:
    (a) to cause death or bodily harm to any person;
    (b) to burn, destroy or damage real or personal property; or
    (c) to kill, poison or injure an animal or bird that is the property of any person.

- **Child Pornography (Section 163.1) [Hybrid Offence]**
  - 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.

- **Making Child Pornography**
  - (2) Every person who makes, **prints, publishes or possesses for the purpose of publication any child pornography** is guilty of:
    (a) an indictable offence and liable to imprisonment for a term not exceeding ten 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 not exceeding two years less a day and to a minimum punishment of imprisonment for a term of six months.

- **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:
    (a) an indictable offence and liable to imprisonment for a term not exceeding ten years and to a minimum punishment of imprisonment for a term of one year; or
    (b) an offence punishable on summary conviction and liable to imprisonment for a term not exceeding eighteen months and to a minimum punishment of imprisonment for a term of ninety days.

- **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 five years and to a minimum punishment of imprisonment for a term of six months; or
    (b) an offence punishable on summary conviction and is liable to imprisonment for a term of not more than 18 months and to a minimum punishment of imprisonment for a term of 90 days.

- **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 five years and to a minimum punishment of imprisonment for a term of six months; or
    (b) an offence punishable on summary conviction and is liable to imprisonment for a term of not more than 18 months and to a minimum punishment of imprisonment for a term of 90 days.

In consideration of the Coordinating Committee of Senior Officials (CCSO) Working Group's *Report to the Federal/Provincial/Territorial Ministers Responsible for Justice and Public Safety (June 2013)*, SST and their project partners compiled the following as avenues for prosecution within the Criminal Code that are available as viable means to respond to cyberbullying behaviour that has become criminal due to the elements of the offence:

- **Voyeurism (Section 162) [Hybrid Offence]**
  - 162 (1) Every one commits an offence **who, surreptitiously, observes** - including by mechanical or electronic means - **or makes a visual recording** of a person who is in circumstances that give rise to a reasonable expectation of privacy, if:
    (a) the person is in a place in which a person can reasonably be expected to be nude, to expose his or her genital organs or anal region or her breasts, or to be engaged in explicit sexual activity;
    (b) the person is nude, is exposing his or her genital organs or anal region or her breasts, or is engaged in explicit sexual activity, and the observation or recording

is done for the purpose of observing or recording a person in such a state or engaged in such an activity; or

(c) the observation or recording is done for a sexual purpose

(2) Definition of "visual recording":

In this section, "visual recording" includes a photographic, film or video recording made by any means.

- **Publication, etc., of an intimate image without consent (Section 162.1) [Hybrid Offence]**
  - 162.1 (1) Everyone who knowingly publishes, distributes, transmits, sells, makes available or advertises an intimate image of a person knowing that the person depicted in the image did not give their consent to that conduct, or being reckless as to whether or not that person gave their consent to that conduct, is guilty
    a) of an indictable offence and liable to imprisonment for a term or not more than five years; or
    b) of an offence punishable on summary conviction

    (2) In this section, “Intimate image” means a visual recording of a person made by any means including a photographic, film, or video recording,
    (a) in which the person is nude, is exposing his or her genital organs or anal region or her breasts or is engaged in explicit sexual activity;
    (b) in respect of which, at the time of the recording, there were circumstances that gave rise to a reasonable expectation of privacy; and
    (c) in respect of which the person depicted retains a reasonable expectation of privacy at the time the offence is committed.

- **Luring a Child (Section 172.1) [Hybrid Offence]**
  - 172.1 (1) Every person commits an offence **who, by a means of telecommunication**, **communicates with**
    (a) a person who is, or who the accused believes is, under the age of 18 years, for the purpose of facilitating the commission of an offence under subsection 153(1), section 155, 163.1, 170 or 171 or subsection 212(1), (2), (2.1) or (4) with respect to that person;
    (b) a person who is, or who the accused believes is, under the age of 16 years, for the purpose of facilitating the commission of an offence under section 151 or 152, subsection 160(3) or 173(2) or section 271, 272, 273 or 280 with respect to that person; or
    (c) a person who is, or who the accused believes is, under the age of 14 years, for the purpose of facilitating the commission of an offence under section 281 with respect to that person.

- **Intimidation (Section 423) [Hybrid Offence]**
  - 423. (1) Everyone is guilty of an indictable offence and liable to imprisonment for a term of not more than five years or is guilty of an offence punishable on summary conviction who, wrongfully and without lawful authority, for the purpose of **compelling another person to abstain from doing anything** that he or she has a lawful right to do, or to do anything that he or she has a lawful right to abstain from doing,

(a) **uses violence or threats of violence** to that person or his or her spouse or common-law partner or children, or injures his or her property;
(b) **intimidates or attempts to intimidate that person** or a relative of that person by threats that, in Canada or elsewhere, violence or other injury will be done to or punishment inflicted on him or her or a relative of his or hers, or that the property of any of them will be damaged;
(c) persistently follows that person;
(d) hides any tools, clothes or other property owned or used by that person, or deprives him or her of them or hinders him or her in the use of them;
(e) with one or more other persons, follows that person, in a disorderly manner, on a highway;
(f) besets or watches the place where that person resides, works, carries on business or happens to be; or
(g) blocks or obstructs a highway.

- Exception
  (2) A person who attends at, or near, or approaches a dwelling-house or place, for the purpose only of obtaining or communicating information, does not watch or beset within the meaning of this section.

- **Mischief in Relation to Data (Section 430 (1.1) [Hybrid Offence]**
  - 430 (1.1) Every one commits mischief who wilfully
    (a) destroys or alters data;
    (b) renders data meaningless, useless or ineffective;
    (c**) obstructs, interrupts or interferes with the lawful use of data**; or
    (d) obstructs, interrupts or interferes with any person in the lawful use of data or denies access to data to any person who is entitled to access thereto.

- **Unauthorized Use of Computer (Section 342.1 (1) [Hybrid Offence]**
  - 342.1 (1) Everyone who, fraudulently and without color of right,
    (a) obtains, directly or indirectly, any computer services,
    (b) by means of an electro-magnetic, acoustic, mechanical or other device, intercepts or causes to be intercepted, directly or indirectly, any function of a computer system,
    (c) uses or causes to be used, directly or indirectly, a computer system with intent to commit and offence under paragraph (a) or (b) or an offence under section 430 in relation to data or a computer system, or
    (d) **uses, possesses, traffics in or permits another person to have access to a computer password that would enable a person to commit an offence** under paragraph (a), (b), or (c)

- **Identity Fraud (Section 403 (1) [Hybrid Offence]**
  - 403. (1) Everyone commits an offence who fraudulently personates another person, living or dead,
    (a) with intent to gain advantage for themselves or another person;
    (b) with intent to obtain any property or an interest in any property;

(c) **with intent to cause disadvantage to the person being personated** or another person; or

(d) with intent to avoid arrest or prosecution or to obstruct, pervert or defeat the course of justice.

- **Extortion (Section 346 (1) [Indictable Offence]**
  - 346. (1) Every one commits extortion who, without reasonable justification or excuse and with intent to obtain anything, **by threats, accusations, menaces or violence induces or attempts to induce any person**, whether or not he is the person threatened, accused or menaced or to whom violence is shown, **to do anything or cause anything to be done.**

- **False Messages, Indecent and Harassing Telephone Calls (Section 372) [Hybrid and Summary Convictions respectively]**
  - 372. (1) False messages - Everyone who, with intent to injure or alarm any person, **conveys or causes or procures to be conveyed** by letter, telegram, telephone, cable, radio or otherwise information that he knows is false is guilty of an indictable offence and liable to imprisonment for a term not exceeding two years.

    (2) Indecent telephone calls - Everyone who, with intent to alarm or annoy any person, makes any **indecent telephone call** to that person is guilty of an offence punishable on summary conviction

    (3) Harassing telephone calls - Everyone who, without lawful excuse and with intent to harass any person, makes or causes to be made **repeated telephone calls** to that person is guilty of an offence punishable on summary conviction

- **Counselling or Aiding Suicide (Section 241) [Indictable Offence]**
  - 241. Everyone who

    (a) **counsels a person to commit suicide**, or

    (b) aids or abets a person to commit suicide,

    Whether suicide ensues or not, is guilty or an indictable offence and liable to imprisonment for a term not exceeding fourteen years.

- **Defamatory Libel (Section 298-301) [Indictable Offence]**
  - 298. (1) Definition - A "**defamatory libel**" is matter published, without lawful justification or excuse, that **is likely to injure the reputation of any person** by exposing him to **hatred, contempt or ridicule**, or that is designed to insult the person of or concerning whom it is published.

    (2) **Mode of expression** - A defamatory libel may be expressed directly or by insinuation or irony

    (a) in words legibly marked upon any substance

    (b) by any object signifying a defamatory libel otherwise than by words.

    299. **Publishing** - a person publishes a libel when he

    (a) exhibits it in public,

    (b) causes it to be read or seen, or

(c) shows or delivers it, or causes it to be shown or delivered, with intent that it should be read or seen by the other person whom it defames or by any other person.

300. **Punishment of libel known to be false** - Everyone who publishes a defamatory libel that he knows is false is guilty of an indictable offence and liable to imprisonment for a term not exceeding five years.

301. **Punishment for defamatory libel** - Everyone who publishes a defamatory libel is guilty of an indictable offence and liable to imprisonment for a term not exceeding two years.

- **Public Incitement of Hatred (Section 319) [Hybrid Offence]**
  - 319 (1) **Public Incitement of Hatred** - Everyone who, by communicating statements in any public place, incites hatred against any identifiable group where such incitement is likely to lead to a breach of the peace is guilty of a [Hybrid Offence]

(2) **Wilful Promotion of Hatred** - Everyone who, by communicating statements, other than in private conversation, wilfully promotes hatred against any identifiable group is guilty of [Hybrid Offence]

- **Assault (Section 265) [Hybrid Offence]**
  - 265 (1) A person commits an assault when

(a) without the consent of another person, he applies force intentionally to that other person, directly or indirectly

(b**) he attempts or threatens,** by an act or a gesture, to apply force to another person, if he has, or causes that other person to believe on reasonable grounds that he has, present ability to effect his purpose; or

(c) while openly wearing or carrying a weapon or an imitation thereof, he accosts or impedes another person or begs

(2) **Application** - This section applies to all forms of assault, including sexual assault, sexual assault with a weapon, threats to a third party or causing bodily harm and aggravated sexual assault.

Another Avenue for Reporting Cyberbullying

The Office of the Privacy Commissioner of Canada (OPC) provides Canadians with another avenue to combat cyberbullying by ensuring that their privacy rights are maintained and respected by both private and public sector companies. The OPC oversees compliance with two pieces of federal legislation: the *Privacy Act* (relating to public sector government agencies), and the *Personal Information Protection and Electronic Documents Act* (PIPEDA) which is Canada's private sector privacy law. PIPEDA allows individuals to complain about privacy violations by private sector companies (such as Facebook, Twitter, and Instagram). Complaints as an individual can be made through their website at http://www.priv.gc.ca/ and a copy of the complaint form has been attached in Appendix F.

The Commissioner focuses on resolving complaints through negotiation and persuasion, using mediation and conciliation in appropriate cases. However, if voluntary co-operation is not forthcoming, the Commissioner has the power to summon witnesses, administer oaths and compel the production

of evidence. In cases that remain unresolved, the Commissioner may take the matter to Federal Court to rectify the situation. Individuals have access to these various remedies through the OPC in cases where criminal charges do not proceed and/or where the service provider refuses to remove the contents.

Updated Legislative Provisions and Relevant Case Law

The following legislative provisions in Canada, outside of the Criminal Code, address bullying. It is particularly interesting to note that all of these Acts are in relation to Education with the exception of Nova Scotia which utilized the Cyber Safety Act. There are no current legislative provisions in the Province of British Columbia.

B.C. has implemented the provincial Expect Respect and A Safe Education (ERASE) comprehensive prevention and intervention strategy. There are 10 key components to the strategy, which includes a multi-level training program for educators and community partners to help them proactively identify and address bullying and other harmful behaviors – whether online, at school or in the community. The importance of having school Codes of Conduct translate into action is an integral part of the ERASE training. Schools are sharing positive strategies on how they are translating policy into action. The training also supports the development of Violence Threat Risk Assessment (VTRA) protocols.

Provincial and Territorial Laws

Several provinces and territories have laws specifically dealing with online and offline bullying:

Ontario: The *Education Act* now includes a specific definition of “bullying”:
"Bullying" means aggressive and typically repeated behaviour by a pupil where,

(a) the behaviour is intended by the pupil to have the effect of, or the pupil ought to know that the behaviour would be likely to have the effect of,

(i) causing harm, fear or distress to another individual, including physical, psychological, social or academic harm, harm to the individual's reputation or harm to the individual's property, or

(ii) creating a negative environment at a school for another individual, and

(b) the behaviour occurs in a context where there is a real or perceived power imbalance between the pupil and the individual based on factors such as size, strength, age, intelligence, peer group power, economic status, social status, religion, ethnic origin, sexual orientation, family circumstances, gender, gender identity, gender expression, race, disability or the receipt of special education.

The following definition of cyberbullying is also given:
(1.2) Without limiting the generality of the definition of “bullying” in subsection (1), bullying includes bullying, known as cyberbullying, that is done through any form of electronic means using any technique, including,

(a) creating a web page or a blog in which the creator assumes the identity of another person;

(b) impersonating another person as the author of posted content or messages; and
(c) communicating material to more than one person or posting material on an electronic medium that may be accessed by one or more persons.

The amended Act also requires schools to provide "instruction on bullying prevention during the school year for every pupil," "remedial programs designed to assist victims of bullying" and "professional development programs that are designed to educate teachers in schools within its jurisdiction about bullying and strategies for dealing with bullying." Each school board is also required to "establish a bullying prevention plan for bullying in schools within the board's jurisdiction."

Quebec: *An Act to prevent and stop bullying and violence in schools* modifies the *Education Act* and *The Act Respecting Private Education*. It defines bullying as "any behaviour, speech, actions or gestures, including cyberbullying, expressed directly or indirectly, in particular through social media, having the aim of injuring, hurting, oppressing or ostracizing an individual". School boards are required to create anti-bullying plans and all school staff must take part in the plan.

Alberta: The *Education Act* was revised in 2012 to define bullying as "repeated and hostile or demeaning behaviour by an individual in the school community where the behaviour is intended to cause harm, fear or distress to one or more other individuals in the school community, including psychological harm or harm to an individual's reputation." The Act requires students to "refrain from, report and not tolerate bullying or bullying behaviour directed toward others in the school, whether or not it occurs within the school building, during the school day or by electronic means," while school boards must "establish, implement and maintain a policy respecting the board's obligation under subsection (1)(d) to provide a welcoming, caring, respectful and safe learning environment that includes the establishment of a code of conduct for students that addresses bullying behaviour." Alberta's law is notable because it requires students to report cyberbullying if they witness it, with penalties including suspension and expulsion possible for those who do not.

Nova Scotia: In 2013 the province legally defined bullying as "behaviour, typically repeated, that is intended to cause or should be known to cause fear, intimidation, humiliation, distress or other harm to another person's body, feelings, self-esteem, reputation or property, and can be direct or indirect, and includes assisting or encouraging the behaviour in any way" and cyberbullying as "bullying by electronic means that occurs through the use of technology, including computers or other electronic devices, social networks, text messaging, instant messaging, websites or e-mail." The *Cyber-Safety Act* lets targets of cyberbullying apply for "protection orders" that may put limits on perpetrators' actions or make them identify themselves, and makes parents of perpetrators responsible for their child's actions if the perpetrator is fewer than 18.

New Brunswick: Section 1 of the *Education Act* includes both online and offline bullying in its definition of "serious misconduct." Students are also guaranteed a "positive learning and working environment" free from "bullying, cyberbullying, harassment and other forms of disruptive or non-tolerated behaviour or misconduct, including behaviour or misconduct that occurs outside school hours and off the school grounds to the extent the behaviour or misconduct affects the school environment." Principals are required to develop a positive learning and working environment plan and to report any incident of serious misconduct to the superintendent of the school district. Each school also must have a Parent

School Support Committee that advises the principal on how to promote respectful behavior and prevent misconduct, helps to develop policies on how to prevent disrespectful behaviour or misconduct and how to support both those students who have participated in disrespectful behaviour and those who have been affected by it.

Manitoba has passed Bill-18 - *Public Schools Amendment Act* (Safe and Inclusive Schools) which has defined bullying in a way that specifically includes cyberbullying, and requires schools to have a written Acceptable Use Policy and a written policy "concerning respect for human diversity" and requires teachers and other school staff to report cyber bullying to their principal, and will apply to anyone who "intentionally assists or encourages the bullying behaviour in any way" as well as the original perpetrator. (Source: MediaSmarts).

Relevant Case Law

Here are some case summaries illustrating the response of the Canadian justice system to bullying and cyberbullying behaviours:

- In *Regina v. Fader*, 2009 BCPC 61, the accused was found guilty of **criminal harassment** for conduct that included sending sexually explicit pictures and videos of the complainant to the complainant's new boyfriend, threatening to send nude pictures of her to numerous people who knew her, and posting pictures of her and her contact information on an adult dating website, which resulted in people contacting her. The judge found that the accused was motivated by jealousy and anger and embarked upon a course of conduct, the motive of which was to make her life miserable."

- In the case of *Regina v. T.C.D.*, 2012 ABPC 338, the accused turned 18-years-old one day after her co-accused, a male young offender, distributed nude photographs of the 14-year-old female complainant. The accused and complainant were friends until they both got involved with the co-accused. The co-accused had received nude photographs of the complainant by text. After the complainant and co-accused had a falling out, the accused provided the co-accused with the names and phone numbers of the people at her school to be sent the photographs, and later attended the complainant's high school for the purpose of bullying her by taunting her and calling her names. The judge found that this caused the complainant to fear for her safety. The accused entered a guilty plea to the charge of **criminal harassment**, and the Crown withdrew the charges relating to **child pornography**. The Crown characterized the situation as one of bullying, and the judge accepted as an aggravating factor in sentencing the Crown's submissions that this form of criminal harassment by people sending nude photographs to other people is becoming more and more prevalent in schools, noting further that this is criminal activity occurring in the community at large. The accused was given a suspended sentence and placed on probation for 12 months.

- In the case of *Regina v. Schultz* [2012] the accused was 20 years old and the complainant was 16 years old when they had a relationship and photographed themselves posing and engaging in various sexual acts. After the relationship ended, the accused posted on a social

networking site, Nexopia, the complainant's age, full name and offered to provide nude photographs to anyone who asked for them. He subsequently posted nude photographs of her on his webpage on several occasions to embarrass and humiliate her. The complainant had some of the images removed by contacting Nexopia and deleting them herself. She also contacted the RCMP and filed a complaint. The accused pled guilty to one count of **transmitting child pornography** and was sentenced to 12 months incarceration followed by 2 years' probation.

- Similarly, in *Regina v. Walsh*, 2006 CanLII 7393 (Ont. C.A.), the accused was 22 years old at the time he took photographs of the 15 year old complainant and himself engaging in consensual sex. The complainant later terminated their relationship. The accused was devastated by this and proceeded to make a collage of photographs of the complainant, including graphic sexual pictures that showed her face but not his, and which included her name and place of residence. He e-mailed the collage to various friends and acquaintances of the complainant. He also saved it in a shared folder on two peer-to-peer sharing programs. A friend of the complainant maliciously e-mailed the collage to the complainant's father, and a student at her school placed a printed copy of the collage in her locker. The accused pleaded guilty to the **making and distribution of child pornography**. The Court of Appeal reduced his initial sentence of incarceration for 2 years followed by 3 years' probation with time already served (8 months in custody prior to his being granted parole) and the probation order was maintained. The Court of Appeal commented that "the circumstances of the case were vastly different from the typical child pornography case." [83] The Court of Appeal further noted the observations made by the Court when the accused was granted bail that "this is not the more typical situation where an offender is using the Internet as a business or a hobby to view or distribute child pornography. This was a one time, immature and very unfortunate response to a personal life event."

- In *Regina v. M.K.*, [2004] OJ No 2574, the 20 year old accused used his cell phone to take nude pictures of his underage girlfriend without her knowledge. The accused posted those images on his website which caused the complainant to be very distraught. The accused pleaded guilty to the charges of **criminal harassment, mischief to property, mischief in relation to data and distributing child pornography.** The judge found that his conduct was "serious in that it was, at least in part, very intrusive and, in fact, malicious." The accused was sentenced to 6 months imprisonment and 2 years' probation. (This case occurred before the enactment of the offence of voyeurism).

- Regina v. Fearon, 2014 SCC 77 was a leading Supreme Court of Canada case relating to the constitutionality of warrantless law enforcement searches of a cell phone incident to arrest. Two men, one armed with a handgun robbed a merchant as they were loading jewellery into their car. Later that evening they were both arrested and during a pat-down search incident to arrest of one of the accused the police located an unlocked cell phone. Police searched the phone and located a draft text message saying "we did it" and included a photo of the handgun that was later matched as the suspect weapon. At trial, Fearon argued that the police search of his cell phone violated his section 8 charter right (the right to be secure against unreasonable search and seizure) and that the evidence should be excluded. The trial judge convicted Fearon of robbery with a firearm, holding that the police had a reasonable prospect

of securing evidence of the offence for which Fearon was being arrested. The Supreme Court of Canada dismissed Fearon's appeal and upheld his conviction.

Case Law Precedent: Law Enforcement Searches of a Cell Phone Incident to Arrest

The following is excerpted from the decision in (Regina v. Fearon, 2014 SCC 77)

The power to search incident to arrest is extraordinary in that it permits reasonable searches when the police have neither a warrant nor reasonable and probable grounds. That the exercise of this extraordinary power has been considered in general to meet constitutional muster reflects the important law enforcement objectives which are served by searches of people who have been lawfully arrested. This power must be exercised in the pursuit of a valid purpose related to the proper administration of justice and the search must be truly incidental to the arrest.

Like other searches incident to arrest, prompt cell phone searches incident to arrest may serve important law enforcement objectives: they can assist police to identify and mitigate risks to public safety; locate firearms or stolen goods; identify accomplices; locate and preserve evidence; prevent suspects from evading or resisting law enforcement; locate the other perpetrators; warn officers of possible impending danger; and follow leads promptly. Cell phone searches also have an element of urgency, which supports the extension of the power to search incident to arrest.

Safeguards must be added to the law of search of cell phones incident to arrest in order to make that power compliant with s.8 of the *Charter*. Ultimately, the purpose of the exercise is to strike a balance that gives due weight to the important law enforcement objectives served by searches incidental to arrest and to the very significant privacy interests at stake in cell phone searches. Consequently, four conditions must be met in order for the search of a cell phone or similar device incidental to arrest to comply with s.8. First, the arrest must be lawful. Second, the search must be truly incidental to the arrest. This requirement should be strictly applied to permit searches that must be done promptly upon arrest in order to effectively serve the law enforcement purposes. In this context, those purposes are protecting the police, the accused or the public; preserving evidence; and, if the investigation will be stymied or significantly hampered absent the ability to promptly conduct the search, discovering evidence. Third, the nature and the extent of the search must be tailored to its purpose. In practice, this will mean that only recently sent or drafted emails, texts, photos and the call log will, generally, be available, although other searches may, in some circumstances, be justified. Finally, the police must take detailed notes of what they have examined on the device and how they examined it. The notes should generally include the applications searched, the extent of the search, the time of the search, its purpose and its duration. The record-keeping requirement is important to the effectiveness of after-the-fact judicial review. It will also help police officers to focus on whether what they are doing in relation to the phone falls squarely within the parameters of a lawful search incident to arrest.

In Summary: New Test for Cell Phone Search

1. The arrest was lawful
2. The search is truly incidental to the arrest. The police have a reason based on a valid law enforcement purpose to conduct the search
3. The nature and extent of the search was tailored to the purpose of the search
4. The police have taken detailed notes of what they have examined on the device and how it was searched

Current Overview in BC Cases

Although this is not case law, the information below was provided by Youth Probation, MCFD in British Columbia. This information is a good indication of the current justice system climate and what types of "cyberbullying" related cases are being managed by Youth Probation.

In a recent review of British Columbia Youth Probation cases, over twenty cases involving cyberbullying were identified. The majority of cases involved threats made on-line (e.g. Facebook) or via text message, three of which progressed to a physical assault. Four cases involved non-consensual posting of intimate images. At the time the information was gathered, 3 youth were awaiting trial or sentence. Of the others, about half were sentenced to some form of community supervision (e.g. probation), one quarter had been placed on a recognizance/peace bond, and one quarter were the subject of an extra-judicial sanctions agreement.

The "Rules" that no one follows:

Popular Social Media Services	User Minimum Age Agreem
Facebook	13 years old
Twitter / Periscope	No Age Restriction
YouTube	13 years old
Instagram	13 years old
Snapchat	13 years old
Tumblr	13 years old
Whisper	17 years old
Yik Yak	17 years old
Ask.fm	13 years old
Kik	13 years old
Chat Roulette	18 years old
4Chan	18 years old
Reddit	No Age Restriction

The above table reflects the age "limits" that are set out by the various social media companies in their terms of service. These restrictions are based on U.S. Federal Law: *Children's Online Privacy Protections Act (COPPA)* which sets out to protect children under the age of 13 from sharing their personal information online. These services encourage users not to lie about their age when they create an account/use the platform. This age restriction tends to act more as a guideline. It does not tend to be enforced and is easily bypassed by youth 12 and younger. If you look at any of these sites you will see that they dominated by youth, and many are much younger than the mandated age.

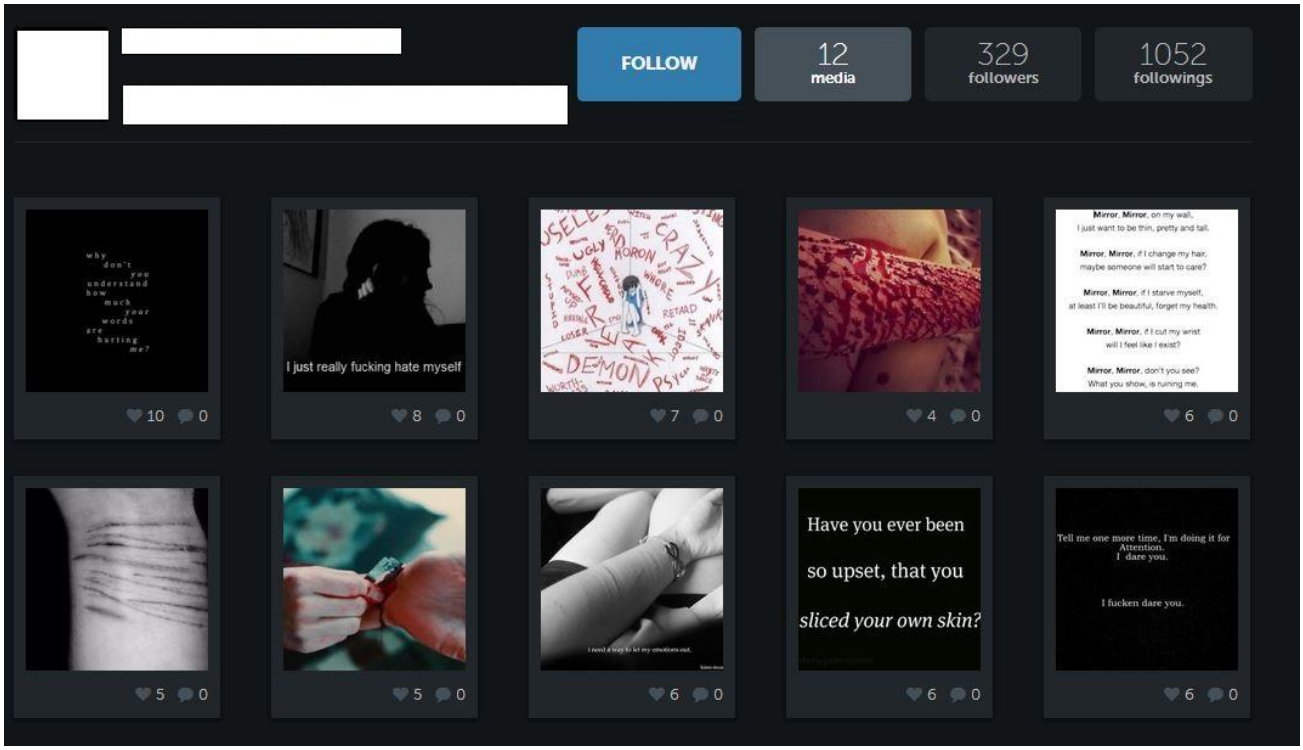
Social Media: The Big Players

Mark Zuckerberg and Facebook recently celebrated their 10 year anniversary as the most popular social network in the world at 1.44 billion monthly active users (up from 100 million in 2008). It has become a household name and still acts as the base hub for most social media activity. Youth are using Facebook less and moving to newer, more popular, ephemeral apps, making it easier to share and connect with friends and strangers. Facebook provides an interesting platform for peer dynamics as "wall communication" is visible to all of a user's friends and peer pressure on Facebook can be no different than the inside of a school hallway. In the post below you will notice how an irrelevant post turns quickly into a conflict.

This Facebook chatter actually manifested into a consensual fight after school the next day.

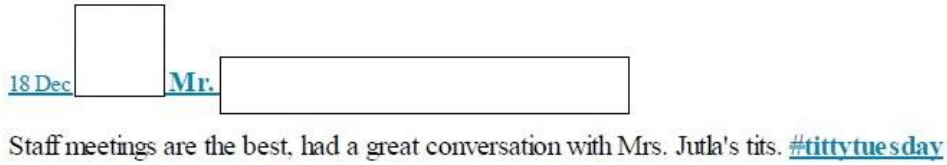
Owned by Facebook, Instagram is the most popular photo-sharing app with over 300 million users. If you see a youth scrolling up with his thumb on their smartphone, chances are they are looking at Instagram. Instagram, like Twitter, can be searched by hashtags (e.g. #suicide) which are then grouped together and this gives people avenues to meet and "follow" other users with similar interests. Instagram is an application built for smartphones. To search Instagram online, the best way is through a web viewer such as www.statigr.am or www.pinsta.me.

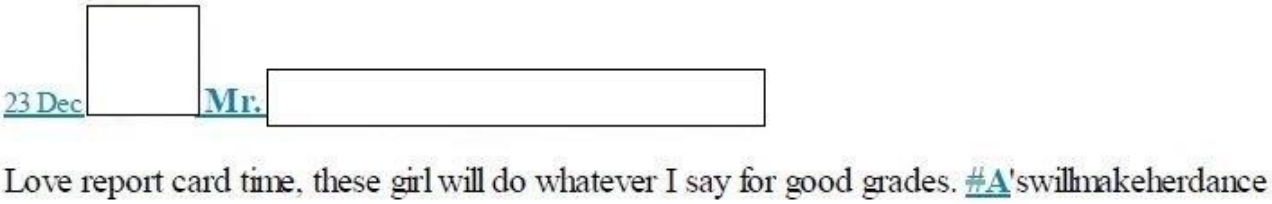
Instagram is a social platform that is a good example of how youth overshare online. To see first-hand, simply search #selfie. Instagram is also one of the many places where youth worrisome behaviour can be found online. Review the profile below of a young girl whose pictures and ideation certainly prompted a closer look. Efforts were taken to identify who was behind the page, and how the individual in the images could be reached and supported.



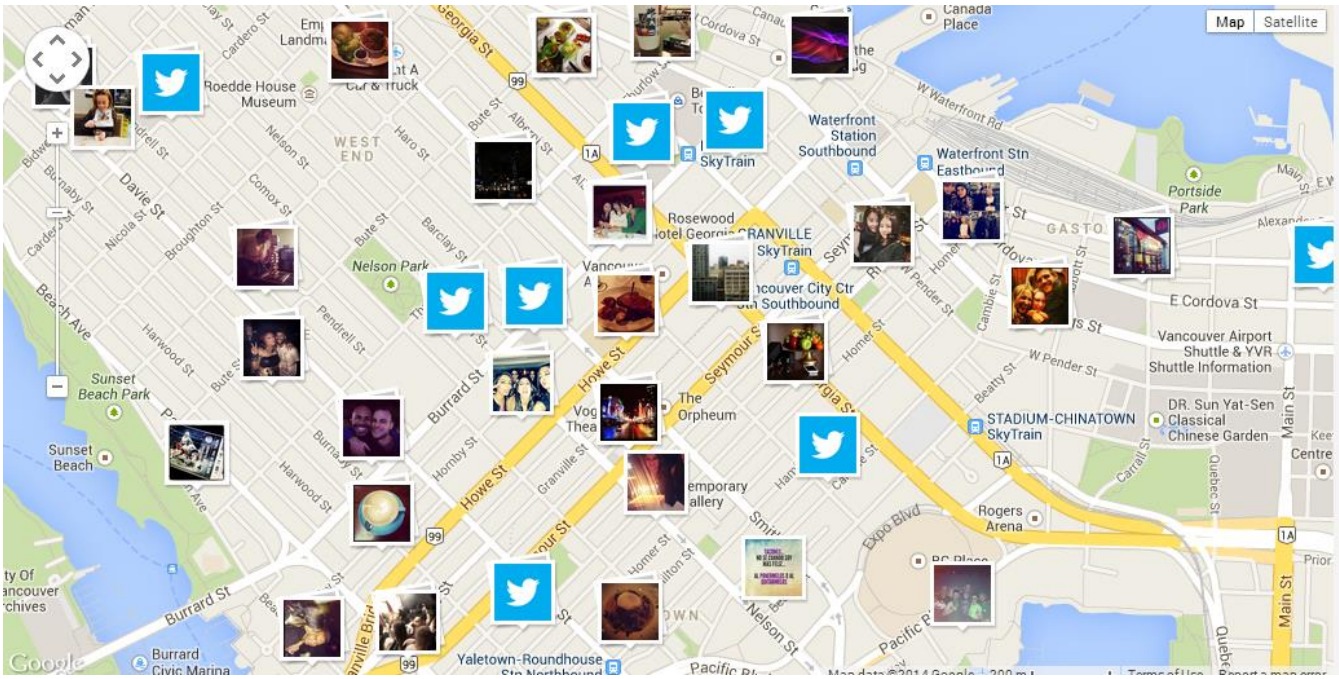
Twitter is the original microblogging network that allows users to post 140-character messages, known as "Tweets" which are can be grouped together and searchable by hashtags (#). Twitter currently has over 300 million monthly active users with upwards of 500 million tweets posted every day. It has become the fastest way for breaking news to travel around the world, so much so that traditional media sources take to Twitter before breaking a story. We are seeing youth using Twitter as a public forum to voice their thoughts and comments. For some youth, this ends up being the every thought. Surprisingly, it is not uncommon to see youth with over 100,000 tweets. Twitter is, by nature, public and prides itself on the freedom of speech, and thus stays far away from mediating disputes between individuals. Twitter generally responds well to requests for the removal of material in relation to impersonation such as the one below.

This was a fake account set up by a student to impersonate his teacher and was used to make inappropriate, damaging and defamatory comments on the teachers' behalf.



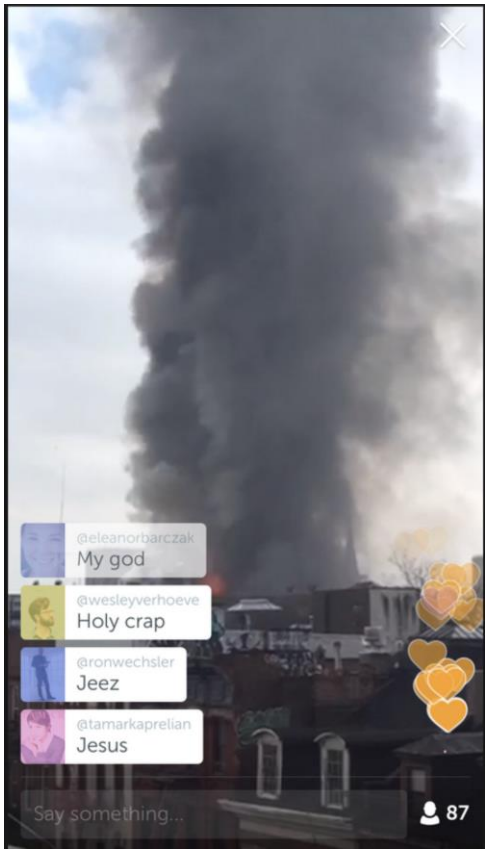


You do not have to look far on Twitter to see that people speak without a filter. Tweets have returned to haunt a range of users from students and parents, to professionals and celebrities. A rule of thumb; if you don't want it on the front page of a newspaper, don't "tweet" it.



An interesting feature, which is incredibly helpful in situations where follow-up is required, is Twitter's geolocational software which allows the user to geo-tag locations. This can then be traced back down to pinpoint the accuracy of a room within a house, in which a "tweet" was generated.

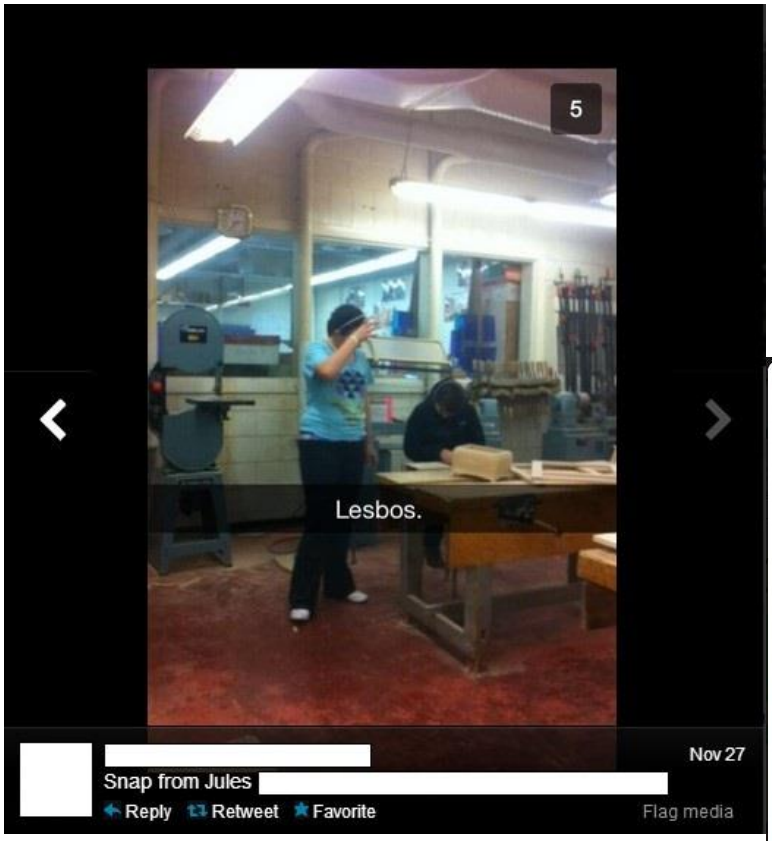
Periscope is one of the latest most popular social media applications to take the market by force. Twitter purchased periscope for $100 million in March 2015 and has since fully integrated it within the traditional Twitter platform as an arm of their market differentiation. The app allows users to live broadcast in real time audio and video of what they are seeing/experiencing through the camera of their smartphone, to an unlimited audience around the world. You can also passively view other video streams shared around the world, comment, see their location, and even save their video stream. As we enter into an era of ubiquitous connectively, Periscope has gained significant market traction by giving citizen journalists, everyday teenagers, and anyone who is curious a platform and stage to share a live broadcast of whatever it may be that they are seeing or experiencing. From a positive standpoint, you can instantly view what people are sharing (and thus seeing) on a beach in Australia or in the mountains of Switzerland. On the negative side, young people who may lack maturity and supervision now find themselves broadcasting to a worldwide audience, and receiving virtually anonymous commentary. We must be cautious to monitor the fact that this commentary has the danger to provide further justification to a young person who may on the pathway to harm themselves and/or others.

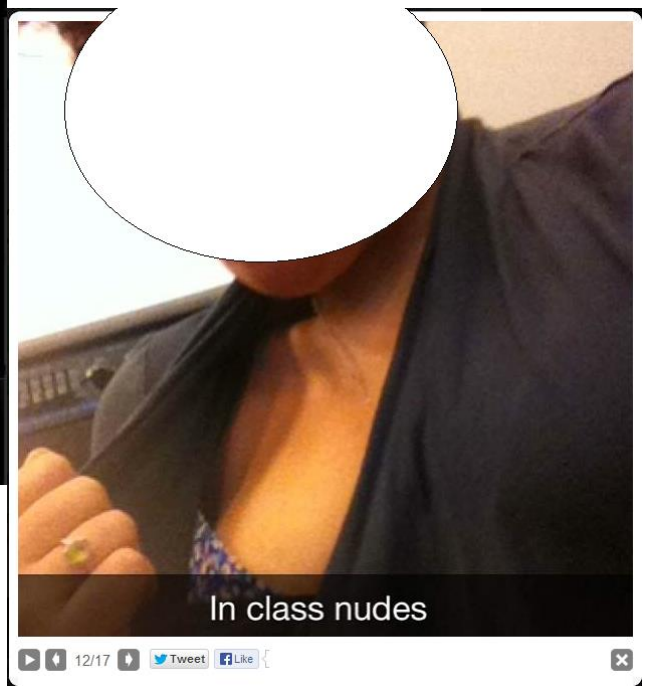


As you can see in this image, a live broadcast of a fire occurring in New York City is streamed to the Internet potentially faster than emergency crews can even begin to mobilize. This showcases how powerful social media can be in connecting users the world over.

Snapchat

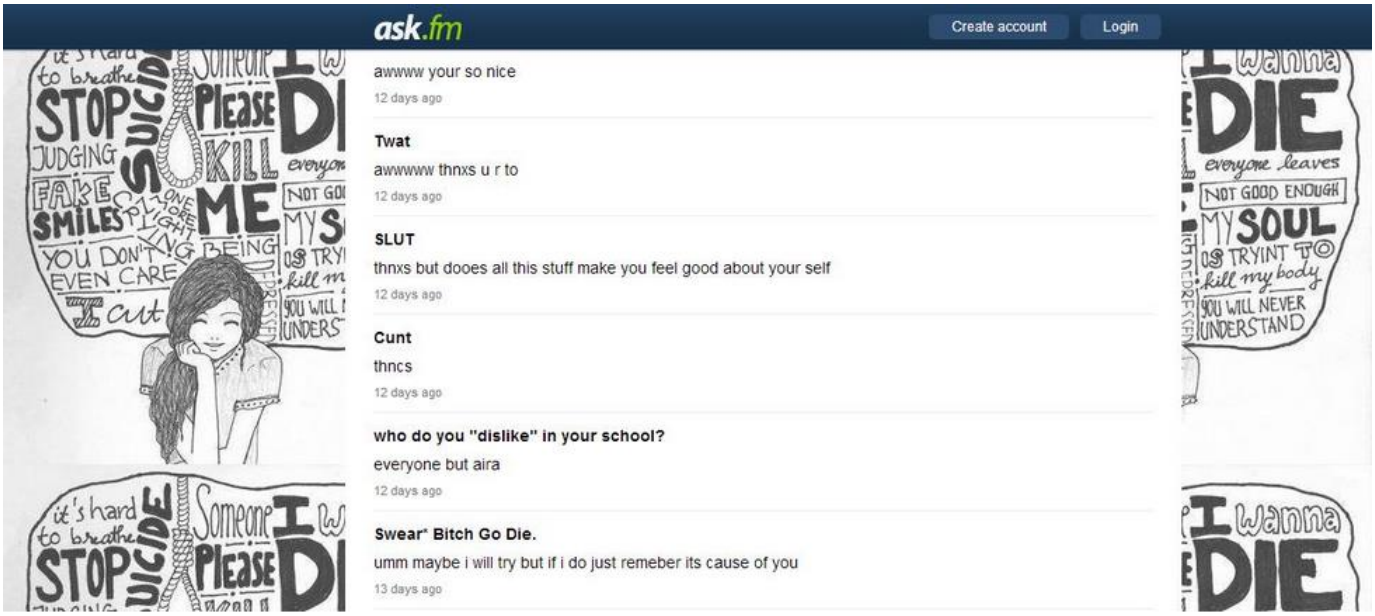
Snapchat is arguably the most popular of applications used by young people in today's digital world. In fact, over 75% of Snapchat's user base is under that age of 25. Launched in 2011, the app sees nearly 400 million Snapchat images sent daily with over 100 million daily users. It is a photo messaging app that allows users to take still photos, record short videos, add text and create drawings and send them to a personalized list of friends. The user sets a viewing time of up to 10 seconds after which, once viewed, it will be deleted from the recipient's device and as the company claims, from its servers. Nothing stops the end user from taking a screenshot or using a camera to take a picture of the image. Given its seemingly temporary and untraceable nature, this is one of the most popular apps among preteens and teenagers for sexting and thus its misuse encompasses exploitation and bullying. The images below are evidence that "snaps" may not disappear, as the image on the left is a screenshot that has been posted to Twitter and the right has been posted to Instagram. You can tell the images were created on Snapchat from the text box across the bottom of the image and the 5 in the corner, which indicates that there are 5 seconds left of viewing before the image "disappears".





Other Apps of Concern

It is a popular question and answer website, and app that allows users to ask questions among one another. The app also allows users to have the option to remain completely anonymous, which of course many youth exercise. It has become the perfect platform for the malicious to bully, harass, and extort someone with essentially no ramifications. Ask.fm is based out of Latvia meaning Canadian law does not apply, making any legal action difficult, if not, futile. Ask.fm has been implicated in at least nine youth suicides around the world. Questions can be as innocent as "Who do you like?" and "What is your favorite subject in school?" However given the anonymity, some youth take advantage and exploit others with malice and hate. The conversations can become highly provocative and sexualized and with little regulation from the site itself, and with little awareness by parents, this results in a dangerous freedom for minds lacking maturity. It is observed across the board there is a general lack of empathy displayed when individuals can hide from behind a screen. An extremely concerning trend that is increasing with the use of ask.fm is the encouragement of making negative comments that are aimed at youth who are depressed and displaying cries for help on ask.fm. Individuals who are looking for positive support from peers are instead recipients of harassment, encouragement to kill themselves, and told that nobody cares about them.



Based on recommendations from a multi-month audit of the service by an international law firm, ask.fm has implemented some positive safety changes: to address the nefarious pitfalls of anonymity users can now "opt out" from receiving anonymous questions. Users can now also report any concerns they have with questions. Ask.fm claims that they are "committed to dealing with any reports of bullying, harassment, or inappropriate questions within 24 hours of a report being made".

Finally, ask.fm moderators will now review every photo and video uploaded to make sure they comply with the terms of use[4]. Although social media dynamites such as aks.fm are beginning to address social and emotional concerns of their users, youth still need to be educated on the appropriate use and content and the consequences of any misuse.

So if anyone asked you to send them nudes would you?

No i dont send them to just anyone

8 days ago

Then who do you send them to?

Boyfriends who i really care out about and really care about me

8 days ago

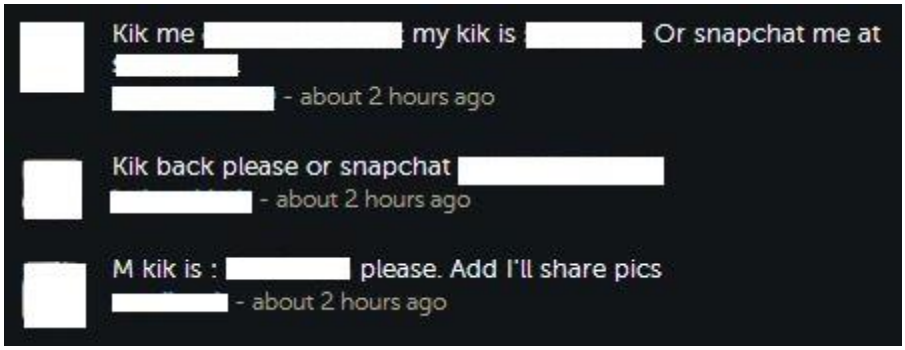
Post a pic of your boobs in the tank top your wearing

Im soo boredddd

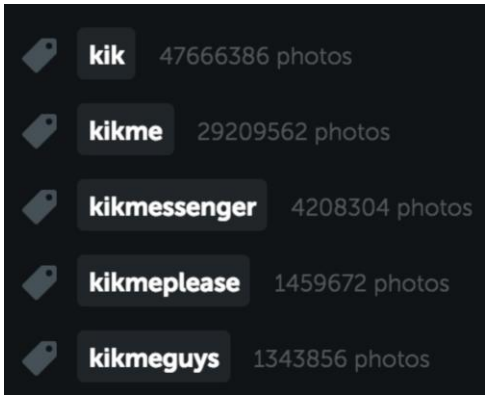
8 days ago

[4] http://www.connectsafely.org/significant-safety-changes-ask-fm/

Kik Messenger, Text + and WhatsApp are all variations on the same communication application – the focus is free phone-to-phone messaging that's private and not applicable to a text messaging (SMS) plan. As it is a cross-platform, and lets you attach pictures and videos, all without counting towards SMS counts or minutes. Parents often think this is a good tool because of the minimal financial impact and the ability to delete the conversation stream. Kik is by far the most popular amongst youth and you will see taglines posted with "kik me", but it can also be the most dangerous because many youth post their kik username online for all to see, which is an easy access lure point for a predator.

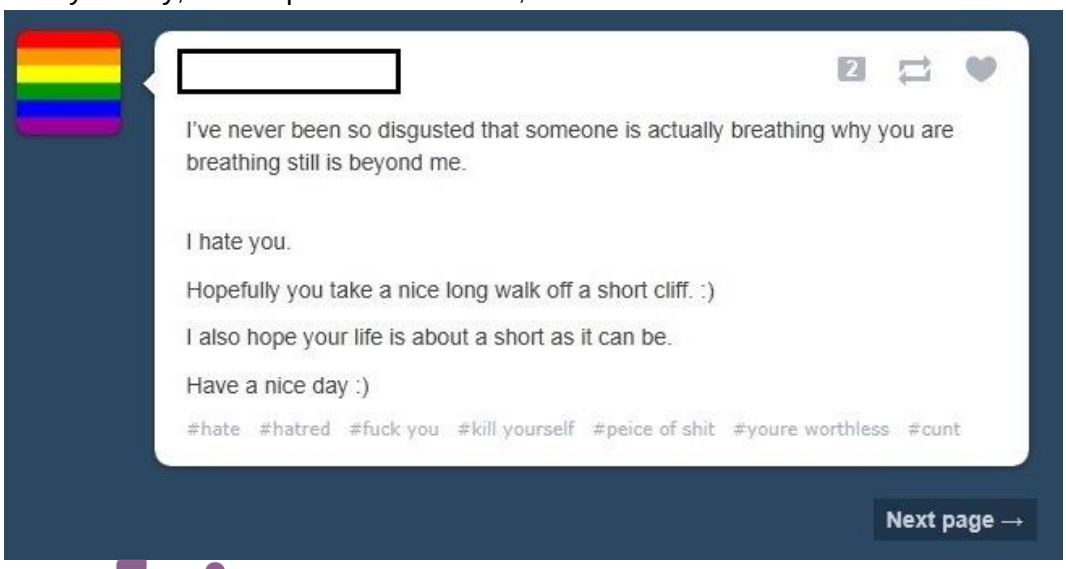


The clip below will give you an idea of how popular Kik is and how it is being used as a tool for youth to communicate with each other, especially when they are bored:

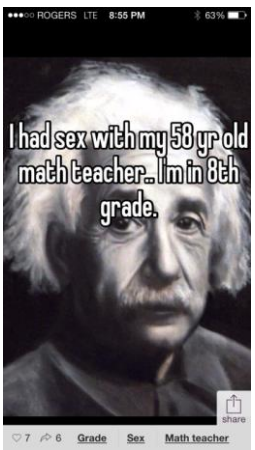


This is from Instagram and how many times #kikme (+47.6 million) and #kikmeplease (1.4 million) has been hashtagged. This means that young people are posting photos on their Instagram accounts, finding others via hashtags and essentially giving their phone numbers (Kik usernames) out to complete strangers.

Tumblr is a blogging platform recently acquired by Yahoo.com for over one billion dollars. This platform is an organized social network appealing to adults and young people “liking” one another's posts, commenting and fielding questions from strangers. Youth like tumblr because they can be expressive and channel their inner feelings, thoughts, and desires into building their own page with backgrounds, pictures, and creativity. Some pages also have a space where comments can be left anonymously, similar premise to ask.fm, where hatred can breed.

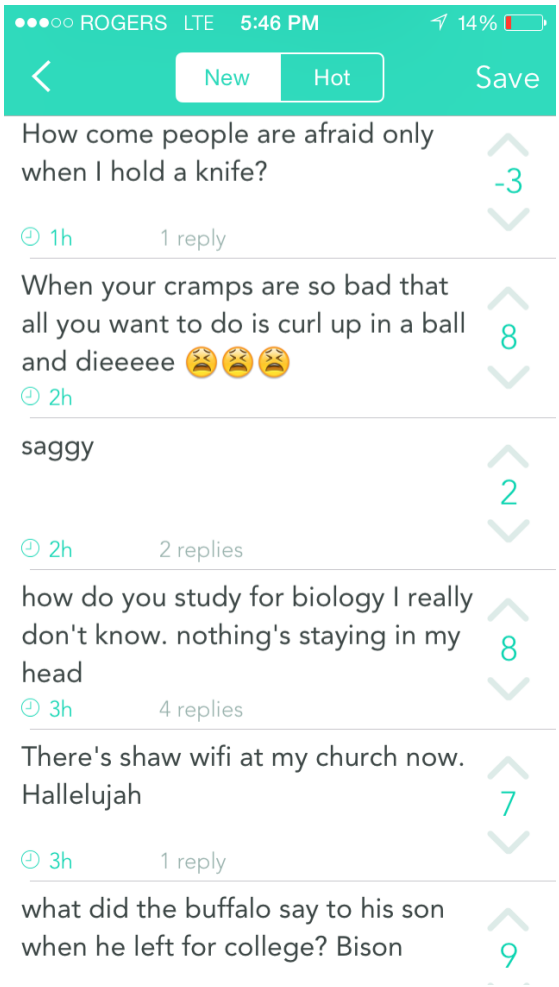


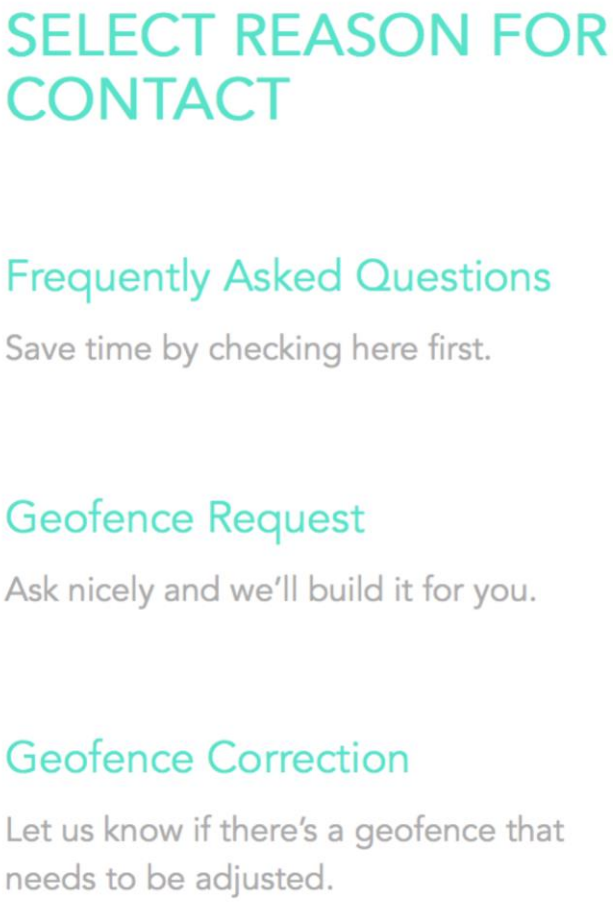
Whisper is a new anonymous social network that gets three billion page views a month and provides a place for young people to share their secrets without the risk of it being traced back to them. It allows users to post written messages on top of photos and illustrations to which other users can like and comment. The idea behind the app is to promote online anonymity and it does a good job doing that. Posts cannot be traced back to a person, and in fact no user data is collected on sign up - only a username. Whisper works on geo-location and presents you with Whispers near your location. This has become another avenue for pre-teens and teenagers to behave inappropriately online, this time securely as "anons" (anonymous).



YIK YAK

Yik Yak is another anonymous based geo-locational app that is surging in popularity among young people. The “Yak” Functions as a comment board by combining GPS technologies and instant messaging allowing users to anonymously view and communicate with other nearby users (1.5 miles). As far as users go, monthly active user estimates fluctuate between 1.7 and 2 million. Given its proximity limitations (1.5 mile radius), with the ability to “peek” or look into other locations around the world, Yik Yak has become a popular app throughout school communities in Canada and the United States. In response to negative use by school aged youth and their app store rating of age 17 and up, Yik Yak has geo-fenced schools around North America to prevent access to the platform on school grounds. Geo fence requests can be submitted at: http://support.yikyakapp.com/





ChatRoulette

www.chatroulette.com is a live online chat website (Not an App) that connects two webcam users randomly from anywhere in the world. From here these users can converse and talk back and forth through their webcam and chat feature. The webcam session can be terminated at any time by either user as they move on to the next random webcam user. This website is a nightmare for parents as kids are instantly connected and virtually interacting with strangers from anywhere in the world. Here, they can be easily led into inappropriate situations where they may be asked to flash or reveal themselves. This is where “screen-cappers”, predators, and pedophiles thrive in an unregulated venue. Omegle is another popular random pairing webcam chat website similar to Chatroulette and is popular among youth.

4Chan is a simple forum platform where anyone can post images and comments on the bulletin boards, hiding behind anonymity, discussions often become hostile and involve extremely dark content. The bulletin boards are categorized into a variety of topics and can be accessed by anyone at any time. As you can see in the “front page of 4chan” image below, adult content is easily accessible to youth, who simply have to click “agree” to continue.

4Chan gained a lot of public attention on Nov 30th, 2013, when a student from the University of Guelph posted a thread on 4Chan stating that he was planning to take his own life that evening. As a long time user of 4Chan, he claimed to want to "give back to the community in the best way possible" by live streaming his suicide. His thread went viral and other 4Chan users supported and further encouraged his plan in a manner akin to counselling suicide.

reddit

www.reddit.com is a social networking website that allows users to share text, pictures, links and news with each other and the reddit "community". Similarly to 4Chan, anyone can view the content but only registered users are able to vote the submission as "Up" or "Down". They are then categorized by popularity and change on a daily basis. Reddit has become a focal point for finding content before it becomes main stream in the media. Submissions and content are organized into subcategories called "subreddits" and these are as diverse as one's imagination. Reddit has been described as the underbelly of the Internet and is the base for a strong contingent of Internet activism. The dark side of reddit is notoriously grotesque with categories as sinister as: r/rapebait, r/incest, r/picsofdeadkids, r/chokeabitch, r/beatingwomen, r/hitler, r/rape.

The subreddit r/jailbait gained international attention when its founder and moderator Michael Brutsch was outed online and publicly targeted. He dedicated this subreddit to sexualized images of underage girls – often referred to by the self-explanatory term "Jailbait". Users posted snapshots of tween and teenage girls, often in bikinis and skirts, many of which were lifted from Facebook pages and thrown in front of Jailbait's 20,000 creepy subscribers. r/jailbait was taken down in October 2011 following a CNN report.

Below is a screenshot of the subreddit – r/suicidewatch

The bottom line is that parents should be very worried if their child is visiting and participating in unregulated sites such as 4Chan and Reddit.

Negative Online Youth Culture Trend: "Cappers" and "Capping"

Cappers are online opportunists/predators and pedophiles who convince girls and young women via online communication, webchats, and Facebook, to take their clothes off and pose for a camera and/or webcam. These images are saved and sometimes used at a later point to extort either another "show" or to distribute amongst their friends or worse – posted online for the world to see on chatrooms and websites such as 4chan or Reddit. Screenshots can be captured as easily as pushing the "Print Screen" button and a digital image is produced in milliseconds.

A capper's *modus operandi* usually begins with a casual chat session without webcam, with pressure soon arriving to switch on the webcam. This continues until requests are made to "flash", these requests are usually preceded by compliments or flattery to distract the girl and boost her confidence - "Show your stomach" or "put on a show". Sometimes all they will get is a quick bra flash while other times they get a full-on disrobe or "bate," which is when a girl masturbates on camera. To the capper community, this would be a "win", which they post in forums. Cappers will also steal bathing-suit photographs from unsuspecting Facebook pages for their "galleries". This illustrates the importance of privacy settings for young people because before they know it their bikini photo in Hawaii with their family is posted up on 4Chan for all to see. Capping is usually the first step

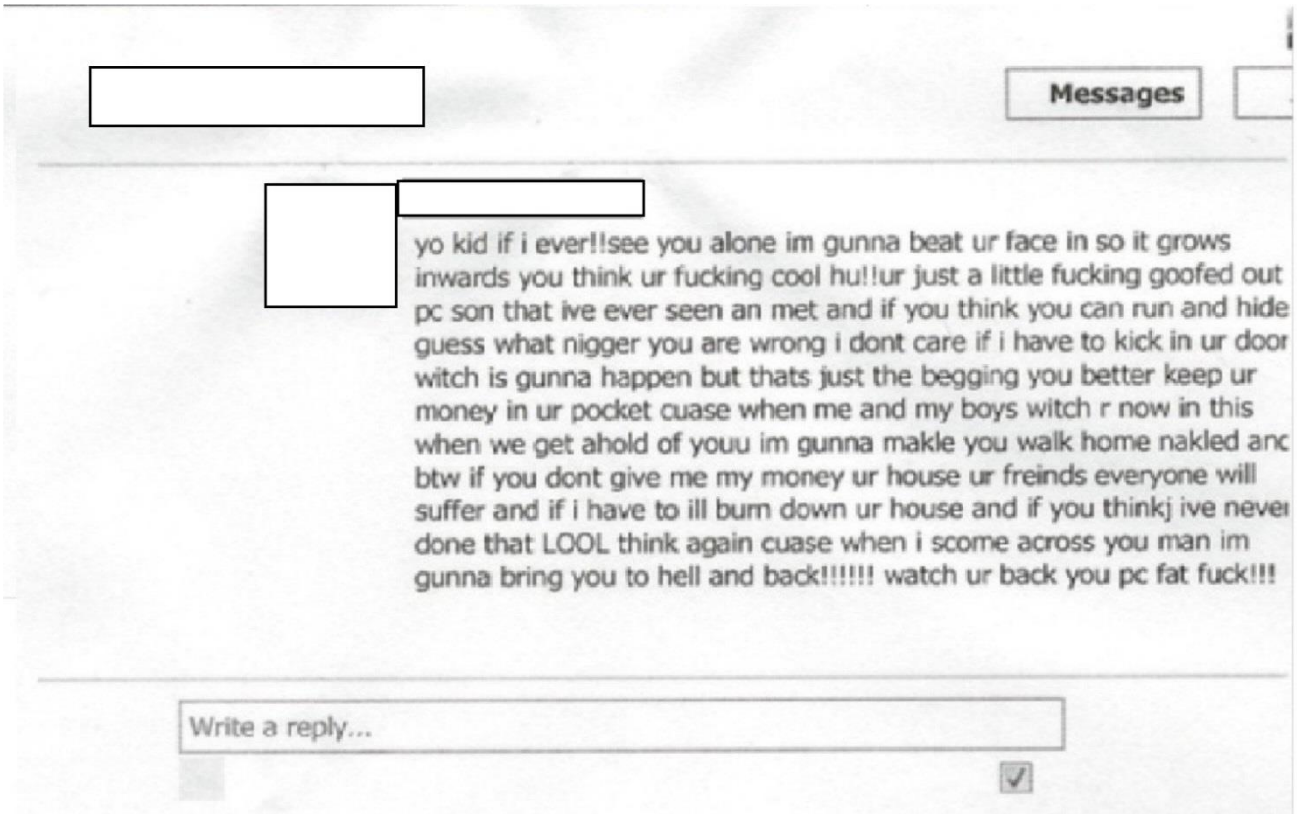
in sexual exploitation and cyber bullying, and can have tragic consequences – Amanda Todd, Jessica Laney and Rehtaeh Parsons well-known examples.

Case Scenarios

Case Scenario 1

Nelson - Grade 6 at Hillside Elementary, 11 years old
Kyle - Grade 7 at Hillside Elementary, 12 years old

Nelson has been bullied by Kyle and his friends for several weeks now; usually they push him down on the walk home after school and call him names. Last night Nelson receives a message from Kyle through Facebook Messenger. Nelson is frightened and comes into the office at the beginning of school and shows the school principal. The school principal prints off the Facebook message and calls the School Police Liaison Officer to attend given the content of the message. You arrive at the school and are handed the following message:



Guiding Questions:

1. What is your next step?

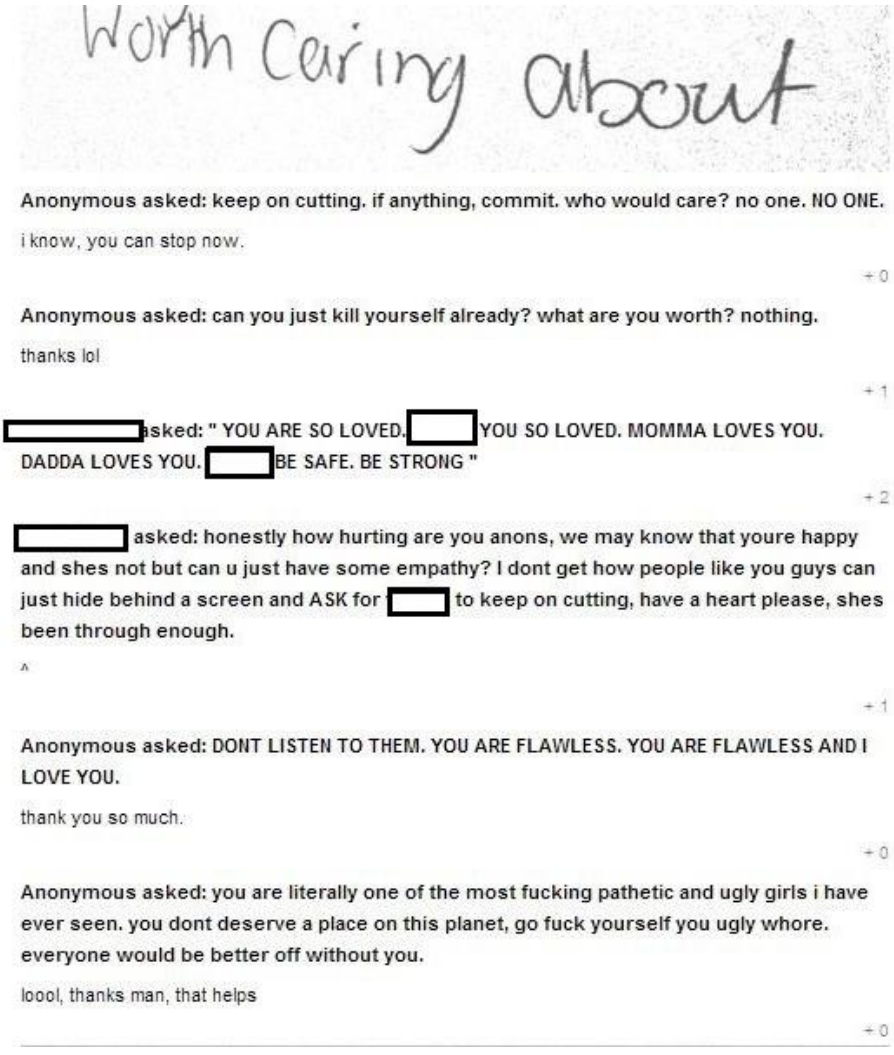
2. How will you search for further information and evidence?

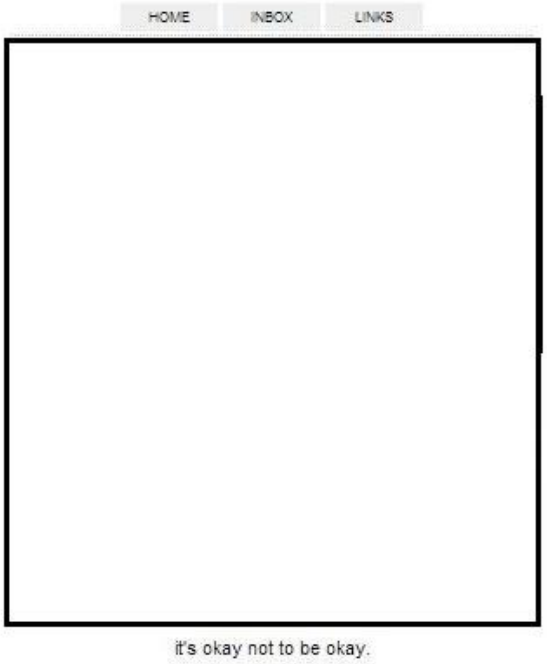
3. What Criminal Code offences do you see within this message?

4. When you interview Kyle he confesses to sending the message. What will you do next?

Case Scenario 2:

You are a Police Officer at a charity hockey game supporting your colleagues playing against a community rep hockey team. A 15 year old boy comes up to you and enquires if he can ask you a question. He tells you that he has heard a rumor that some girl named Alice, two grades below him at his school, is going to kill herself. All he knows is that her name is Alice and that she has a blog. After making a call to the school principal to pass along the information you take it upon yourself to check out her digital footprint, looking for any clues or evidence online. You type in Alice and her school name into Google and find a tumblr blog in the third Google hit. You see this:





Anonymous asked: ur fucking ugly

okay

Anonymous asked: kill yourself please.

sure

Anonymous asked: where do you cut?

i won't tell you for two reasons: you'll look there and it'll give people ideas.

Anonymous asked: have u ever cheated?

no

Anonymous asked: go ahead and kill yourself who cares omg

omg ok

me: i'm sorry, it's just it's been a bad day
me: of a tough week
me: of a bad month
me: of a terrible year
me: of a dreadful existence

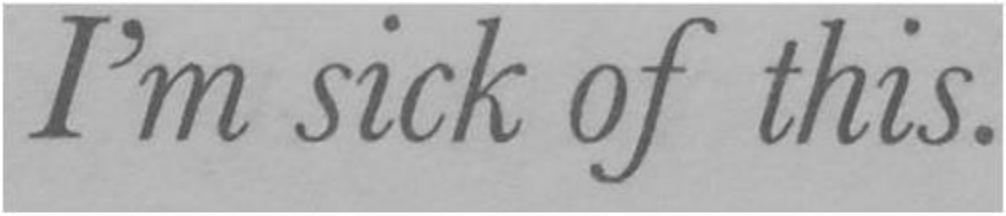
Anonymous asked: pls don't kill urself.. pls.<333

no promises, but ill try not to.

Anonymous asked: you honestly don't deserve what you have or where you are. you are so fucking ungrateful and ugly and stupid and horrendous. this fucking planet is better off without you here so just do us the favor and kill yourself. we don't need you. no one does. so take the fucking hint and kill yourself.

i can't believe you wasted your time typing that out to me. im here and im alive.

+ 0



Anonymous asked: you fucking ugly ass pathetic bitch, go die.

okay

+ 0

Anonymous asked: what are you waiting for? kill. your. self.

i don't know what im waiting for.

+ 2

Guiding Questions:

1. Based on the content above, do you suspect there is a criminal offence? If so, which charges do you see applicable?

2. What are your next steps?

3. Where will you look to investigate Alice's digital footprint?

4. Is this an emergency? "Exigent circumstances"?

5. Where do you see Alice on the suicidal ideation continuum?

Guidelines for Schools & Education

Student safety is the number one priority for school staff. Boards of Education are responsible for ensuring the safety of all students while on school property. They are also responsible for addressing situations where the incident may have occurred off of school property impacting the climate and culture of the school. This is often the case in situations involving cyberbullying.

Challenges

Often school staff are unsure of how to address cyber bullying situations as it can happen at any time, any place – with or without the intended target(s) being aware. In addition, ensuring school staff address incidents without compromising any evidence can pose a significant challenge.

Criminal Code Offence

When a cyberbullying or online incident comes to light, school district staff should begin an initial information collection process (i.e. gathering data, pictures, open source information) unless there is an indication of a Criminal Code offence at which time school staff should contact the School Liaison Officer / Police.

Using Appendix D, Bullying Behaviour Flowchart will help determine if the behaviour or information meets the threshold for a Criminal Code offence, which will assist in when to call or not call the School Liaison Officer / Police to take over the investigation. Note, evidence that has been collected should be preserved and provided to the police. To preserve the evidence take screenshots, save pictures, turn off the mobile device(s), remove the battery, remove the SIM card and place device in airplane mode. Furthermore, do not interview students as this may jeopardize the case should it go to court.

School staff must be aware that as soon as they consult with the police, they have in essence become agents of the police. For example, if the school district staff contacts the School Liaison Officer and asks if a search of a student's locker should occur, they have entered into the realm of an agent. In law enforcement and legal practice, an agent takes direction from the police and must follow a strict set of legal guidelines.

Non-Criminal Code Offence

School staff should continue to gather data using *Appendix E: Bullying Behaviour Checklist*. Gather primary and secondary data including behaviour baselines for the student(s), and also address if and why the behaviour may have changed. A lot of data can be collected at a school level outside of a police investigation. Pay special attention to a student file if it provides any indication of past site or target selection. When digital devices are involved, always follow the same procedure as the police for securing the device whether or not the offence meets the Criminal Code threshold. This includes removing the battery and SIM card, and placing the device into airplane mode. Dealing with mobile

devices in this manner is important as youth have found ways to remotely wipe their devices using alternate devices, such as a school computer or a friend's device.

A non-compliant student who is unwilling to unlock a secured device should be given an opportunity to work with school administration or be referred to the School Liaison Officer. Lastly, when a youth has contravened the Code of Conduct and/or engaged in behaviour that has impacted the school climate and culture, school staff must contact the student's parents or legal guardians as soon as possible.

Restorative Practices in Schools

When schools consider taking a restorative approach to any cases that are not considered criminal matters, there still needs to be a clear understanding of the restorative approach. School-based restorative practice and its' potential for success is largely based on the culture/climate of that particular class/school. Restorative practices are driven by administration, parents and students and the community at large. Employing restorative practices in a school-based environment as a mechanism for maintaining a healthy learning environment requires both human and financial resources, along with training and commitment. In schools, it is meant as an integrated and proactive approach where a major goal is the effective reintegration of students when addressing situations where harm has been done. To parachute restorative practices into an environment where it isn't the expectation or norm, will have limited success. This speaks directly to the importance of ensuring that a school is a naturally open system, with a positive school/class culture and climate as expressed in the BC ERASE strategy. A naturally open system is one whereby school staff collaborates with parents police and community members to keep students healthy, happy and safe. Information sharing in open systems is bi-directional between leadership and other levels of that same system.

Options under the YCJA

The *Youth Criminal Justice Act* (YCJA) provides the legislative framework for dealing with youth accused of criminal offences. It includes specific provisions for dealing with youth outside of the formal court system (diversion), procedural safeguards for youth, and sentencing options for youth.

Terminology

There is confusion regarding terms such as Extrajudicial Measures (EJM), Extrajudicial Sanctions (EJS), diversion and restorative justice. The YCJA places great importance on using non-court processes when addressing youth crime if appropriate. This could include: taking no further action; a warning, caution or referral; or extrajudicial sanctions. All of these are, in fact, extrajudicial measures in the YCJA (Sec 4-12). All of these are, at times, also referred to as "diversion". Restorative Justice is a process where the person who caused harm, and the person who suffered harm, get together in an attempt to repair the harm caused. Within the justice system, restorative justice may be available throughout the continuum of services from referrals to community

programs, youth probation and youth custody. EJM, EJS, and restorative justice are addressed in detail below.

Appropriate use of police discretion in the execution of their duties is of paramount importance to the criminal justice system as a whole. Police officers act as the first responders in the system and as such, the decisions that they make and the discretion that they utilize on the front lines become all that more important. The *Youth Criminal Justice Act* (YCJA) sets out specific principles to guide decision-making at key points in the youth justice process:

"One of the key objectives of the YCJA is to increase the use of effective and timely non-court responses to less serious offences by youth. These extrajudicial measures can provide meaningful consequences, such as requiring the young person to repair the harm done to the victim. They also allow early intervention with young people and provide the opportunity for the broader community to play an important role in developing community-based responses to youth crime. Increasing the use of non-court responses also enables the courts to focus on the more serious cases of youth crime[5] "

When to use extrajudicial measures:

- Extrajudicial measures should be used in all cases where they would be **adequate to hold the young person accountable**.
- Extrajudicial measures are presumed to be adequate to hold first-time, non-violent offenders accountable.
- Extrajudicial measures may be used if the young person has previously been dealt with by extrajudicial measures or has been found guilty of an offence. As amended in 2012, the YCJA requires police to keep records of any extrajudicial measures used with a young person. These records will better inform police so that they can take appropriate action in respect of subsequent alleged offences.

The YCJA requires police officers to consider the use of extrajudicial measures before deciding to initiate formal proceedings against a young person. There is a common belief that many police members think that they *must* use EJM for all youth cases. In reality, they are obligated to *consider it* but they do not have to *use it* unless they feel it is appropriate to hold the young person accountable for their actions. The YCJA also states that failure to consider these options does not invalidate a subsequent charge on the same offence.

a. EJM-Referrals to Community Agency:

A referral may be made to a community agency for the purposes of understanding the underlying causes of the behaviour, providing counsel, education and support to prevent further incidents. The primary goal of these programs is to assist youth in understanding how their behavior affects their family, victim, themselves and the community at large. The main focus of the intervention is to encourage personal responsibility and accountability for their actions. Young people may complete any/all of the following as part of this process:

[5] The *Youth Criminal Justice Act,* Summary and Background, Department of Justice Canada, 2013

- Short-term counselling and/or referral
- Apology letter to the victim
- Attend an education program
- Personal or community service hours
- Restitution
- Community Justice Forum (or other restorative justice format)

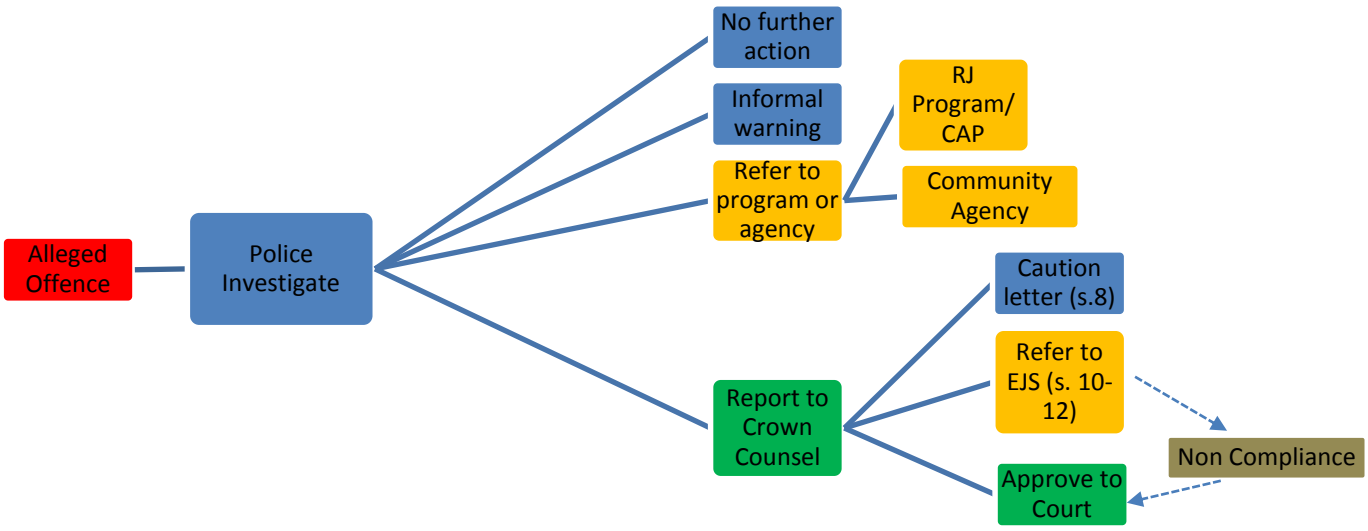
Referrals to community based programs are recorded on PRIME-BC. An individual youth can be referred to community based programs more than one time, and failure to complete EJM does not preclude future referrals on separate matters as long as they are deemed appropriate. In British Columbia, as police members exercising their discretion to refer a youth to a community-based program rather than forwarding a report to Crown Counsel, there is no legal recourse regarding that offence if the youth does not follow through (i.e. you cannot proceed with the original charge or a failure to comply).

b. EJM-Extrajudicial Sanctions (EJS):

As stated above, Extrajudicial Sanctions (EJS) fall within the Extrajudicial Measures provision in the YCJA. EJS can be considered the next "step up" from a warning, caution or referral to a community program and are appropriate if the nature of the offence is such that a warning or a referral to a community program is considered insufficient to hold the youth accountable.

If a young person has already experienced a warning, caution or referral previously and these are NOT considered adequate to hold the young person accountable ***or*** the type of offence is more serious or violent in nature, police can forward a report to Crown Counsel, who have the option to consider Extrajudicial Sanctions. If the Crown Counsel wish to consider EJS in British Columbia, this usually involves a referral to youth probation who will interview the youth and parents and screen the case for appropriateness. Youth probation officers are well trained in the use of EJS and make sure the relevant provisions of the YCJA are followed. After screening the case, youth probation may recommend proceeding with EJS or having the matter dealt with in youth court. The final decision rests with Crown Counsel.

If recommending EJS, youth probation will include a formal plan or agreement which typically involves a three month period of supervision and support provided by a youth probation officer and conditions similar to those listed above. An EJS agreement may also include a therapeutic intervention provided by Youth Forensic Psychiatric Services. Unlike a police referral to a community program, there is a process to address non-compliance with EJS. Although not a "breach", if the young person fails to comply with the terms and conditions of the extrajudicial sanctions agreement, youth probation notifies Crown counsel who may decide to proceed through the court process on the original charge.



c. Formal Charges and Sentences:

If the police have elected not to use a warning, caution, or referral and Crown counsel has elected not to use EJS, the matter will often be dealt with in Youth Court. As noted previously, we have already seen a number of "cyberbullying" cases proceed through Youth Court in BC.

Youth Sentencing

The following is a plain language list of Sentencing Options for young persons who are found guilty of an offence by a Youth Court Justice:

- Reprimand
- Absolute Discharge (if in the best interest of the young person and not contrary to public interest)
- Conditional Discharge (conditions considered appropriate that may require reporting and supervision by a provincial director (i.e. youth probation)
- Fine not exceeding $1000
- Compensation for loss or damage to property, loss of income/support, special damages, personal injury arising from the commission of the offence
- Restitution to victim (fix what was broken)
- Personal Service to victim that may repair any loss, damage or injury suffered by that person
- Community Service Order (hours)
- Prohibition Order (no-go to computers/weapons/drugs etc. based on the details of the offence)
- Probation Order for specified period not exceeding two years
- Intensive Support and supervision Order
- Custody and Supervision Order 2-3 years max. dependent on offence (longer sentences available for murder)
- Deferred Custody and Supervision Order not exceeding six months

Conditions of these Orders often include the following:

- Reporting
- Counseling/education/support
- Restorative Justice/repair of harm done

It is important for all partners to be aware of the options at each stage (Police, Crown and Court) and understand that there are opportunities for resolution throughout the process.

Restorative Justice

Definition and Understanding the Goals

Restorative justice seeks to create just outcomes by repairing the harm done by crime and violence. Typically this happens through facilitating a process that addresses victims' needs and holds offenders meaningfully accountable for their actions. In this approach, crime is understood not only as breaking the law, but as a violation of people and relationships and a disruption of the peace in a community.

Restorative justice is based on an understanding of wrong-doing. The social expectation that follows is that when someone is violated, there is an obligation to put right the wrong-doing. (Adapted from Howard Zehr, Little Book of Restorative Justice, 2002)

Benefits of Restorative Justice

Victims of crime, conflict or wrong-doing have an opportunity to:

- discuss the personal impact an incident has had on them;
- gain a greater understanding of the incident;
- actively participate in a process of determining appropriate reparation; and
- obtain resolution and sometimes closure.

Youth who have caused harm have an opportunity to:

- take responsibility for their actions within the community;
- participate in developing a fair and reasonable agreement with those who were harmed;
- repair harm and make things right with the help of a supportive community; and
- potentially avoid a lengthy court process and criminal record.

For the community, the process provides:

- a more expedient and cost effective alternative to court;
- an opportunity for community involvement and active participation in the judicial process;
- a greater sense of justice defined by accountability, understanding and healing; and
- an opportunity to build stronger and safer communities.

The following are some keys to effective restorative justice practices:

- offender must take responsibility for his/her actions (admit)
- offender must show some level of remorse for their behaviour
- offender must be ready and willing to make efforts to repair the harm
- victim(s) need to be genuinely interested in the process (not feel like it's their only option)
- victims(s) need to be represented (either in person, by representative or by proxy with a victim impact statement/letter/video)
- all parties must freely consent to the process and understand that it is voluntary and that they may withdraw or take a break from the process at any point;
- there needs to be supports in place for each party (offender and victim)
- there needs to be a reintegration plan regarding how each party will move forward from this process and how other people might support the reintegration plan.

RJ is not Appropriate When:

Questions continue to be raised regarding the appropriate use of restorative justice (meaning, community justice forums, healing circles, etc.) when dealing with cyberbullying cases. Broader research is divided on the risks and benefits of using restorative justice in power-based crimes Interviews with a variety of victim services personnel and restorative justice experts indicated the following situations should NOT be handled via restorative practices at this time:

- Domestic violence
- Power-based crimes
- Hate crimes
- Sexual assault
- Serious harassment, intimidation or severe threats

Each case is unique and will require careful consideration of how to proceed. It is imperative that the school or community where the offence takes place is working collaboratively with experienced restorative justice practitioners and victim service agencies.

The term "Restorative Justice" is often used to describe diversion or a community based program that accepts EJM referrals directly from the police. Many of the community agencies that accept referrals from the police in B.C. use a Restorative Justice approach but it is important to know that Restorative Justice is used throughout the continuum of the youth justice system from community based agencies, to youth probation, and in youth custody centres**.**

Guidelines for Police:

Challenges

One of the many challenges we are hearing from frontline police in investigating cyber and online related offences is the lack of knowledge and understanding around the technologies/apps and how they work (e.g. Snapchat and Kik). The fact is that Apps change on a daily basis and it would be helpful to have regular professional development training for police to keep with current technology as it evolves.

Another challenge that plagues police officers investigating a crime anywhere is knowing who the offender(s) is/are. Once the IP address is verified and validated it can still be difficult to know the offender as many people may use the same computer. If it is occurring from a known suspect, be it a youth, there are many hurdles to proceeding with charges - such as a supervisor who would like to see the file referred to a community program and alternative measures used, or a lack of knowledge on the part of crown, police, school staff.

Further, there can be confusion regarding the options available for police officers at the EJM level in BC. As noted, police can take no further action, can give a warning, can give a formal caution (e.g. letter to the young person) or they can refer the young person to a program. These programs can vary by jurisdiction based on services available. Referrals can be made to any of the following: counselling, recreation, substance use, intervention programs (these are typically designed to respond to first-time, non-violent offenders) and restorative justice programs. It is important to note that when a referral is made to restorative justice programs, there is a set of criteria that must be understood and communicated to the young person and their target *prior* to making the referral.

Police Decision Making, Discretion and the YCJA

As a viable option for police officers to advance their knowledge of the *Youth Criminal Justice Act*, the Justice Education Society of BC has launched an online YCJA course for police and professionals, educators and students. In addition, the RCMP offers an Overview of the YCJA, a 2.5 hour course on Agora. This course focuses on the practical application of the YCJA in daily police duties. Municipal police departments can access this course through the Canadian Police Knowledge Network (http://www.cpkn.ca). This course was developed in consultation with the Department of Justice. There is also an updated YCJA Pocket Guide available online.

Police referrals to Community Based RJ Programs: Considerations for Cyberbullying

A referral to a community based restorative justice program is inappropriate when dealing with sexual offences, as discussed above. These referral decisions can be less clear when dealing with the wide array of behaviour referred to as “cyberbullying”. Since cyberbullying itself is not an offence in itself, when dealing with cyberbullying it is necessary to “drill down” and consider the actual behaviour, intentions and the consequences. When we do this, we see clearly that cyberbullying can include offences such as uttering threats, extortion, counselling suicide, criminal harassment, assaults related to online content and/or “sexting”. These behaviours can constitute serious criminal offences resulting in devastating consequences for the victim.

Again, every case is unique and must be considered separately. For example, when we look at the various types of “sexting” cases, it is possible to assume that not all include criminal intentions, (regardless of the fact that the photos shared between minors under the legal age of 18 is Child Pornography, according to current Canadian Law). There are varying approaches to whether youth should be charged with sharing intimate images in a consenting relationship, however, when this normative sexual adolescent behaviour becomes something more based on threats and/or power imbalance in a relationship, it becomes a very serious situation and should be investigated carefully in the criminal context.

If we have a case where an ex-boyfriend is continuously harassing his former girlfriend and demanding that she perform additional acts online and/or provide further intimate images, we are more or less entering the realm of domestic (in this case "dating") violence. Domestic violence is a serious concern and should be directed to Crown Counsel. On the other hand, a 14 year old boy who shares a picture of his girlfriend with another boy, without any malicious intent, can usually be addressed outside of the formal justice system.

To Charge or Not to Charge?

Police officers have difficult decisions to make when dealing with potential youth offences. In non-urgent cases there is an opportunity for them to consult with a local youth probation office or Crown Counsel to help them decide how to proceed. If a warning, caution, or referral is not considered sufficient to hold the young person accountable, a report to Crown Counsel is required.

Things to consider are:

1. seriousness of the offence
2. impact on the victim
3. intention of the young person
4. young person's willingness to take responsibility and make amends
5. young person's history of offences or involvement with police
6. availability of local resources to adequately hold the young person accountable for the offence

It is important to take all these factors into consideration on each case to make the right decisions for all involved. While it is important to follow the intentions of the YCJA and not unnecessarily involve youth in the justice system, it is equally important to identify when cyberbullying incidents constitute a significant offence requiring a formal response.

Youth Statements:

Police investigations relating to allegations of cyberbullying often include statements provided to the police by young persons (under the age of 18 years). The admissibility of these statements is an important issue. Crown Counsel, in their charge assessment function, will be looking carefully at any statements provided by the young person when determining if there is sufficient evidence to support a conclusion that the charge assessment standard has been met.

It is important that police officers investigating cyberbullying cases understand the law relating to the admissibility of youth statements – this includes the relevant legislation and the applicable case law. Members of the RCMP can refer to pages 1 and 2 of the RCMP form ED650 (2013 -05) which contains a Guide to Officers for Section 146 YCJA Statements. Members should also familiarize themselves with Youth Waiver Forms.

Relevant Legislation:

Section 146 of the *Youth Criminal Justice Act* sets out comprehensive rules relating to the admissibility of youth statements. This section starts by acknowledging that the law relating to the admissibility of statements taken from adult offenders is generally applicable to young persons.

Statements, written or oral, will not be admissible unless:

1. the statement was voluntary,
2. it has been clearly explained to the youth person in language appropriate to his/her age and understanding, that
   - he/she was under no obligation to make a statement,
   - the statement may be used as evidence in proceedings against him/her,
   - he/she has the right to consult counsel and a parent or other person, and
   - he/she is entitled to make the statement in the presence of counsel and any other person consulted
3. the youth person has been given a reasonable opportunity to consult
   - counsel, and
   - a parent or an adult relative or any other appropriate adult chosen by the young person, and
   - to have the person they consulted present for the making of the statement

These rigorous requirements do not apply where the young person has given a spontaneous oral statement, s. 146(3) YCJA.

A young person may waive his/her right to consult counsel but such a waiver must either:

1. be recorded, or
2. be in writing and signed by the young person,

If there has been a technical irregularity, a youth justice court may admit the statement if it is satisfied that "the admission of the statement would not bring into disrepute the principle that young persons are entitled to enhanced procedural protection to ensure that they are treated fairly and their rights are protected", s. 146(5) YCJA.

If there is any chance that the young person may be accused of committing an offence s. 146 YCJA should be complied with.

Relevant Case Law:

Regina v. S.S. [2007] (Ont.C.A.) 481. Stands for the proposition that s. 146(2)(b)(iv) requires that the person(s) the youth consult prior to providing a statement must be present unless the youth desires otherwise.

Regina v. Z.(D.A.), [1992] 2 S.C.R. 1025 (SCC). Where an offender is alleged to have committed an offence as a youth person but has passed his eighteenth birthday at the time of police questioning the requirements under s. 146 YCJA do not need to be complied with.

Regina v. L.T.H., [2008]2 S.C.R. 739 (SCC). The Crown is not required to prove that the young person actually understood the caution provided but only that the explanation must be in language appropriate to the young person's age and understanding.

Best Practices:

1. Determine if the person you are dealing with is a "young person" (under 18 years old).

2. Determine if this person is a possible suspect and if he/she is treat him/her as a "young person" within the meaning of the YCJA.
3. Determine if you wish to obtain a statement from this "young person".
4. If you do, arrange to have recording equipment available and advise the young person that the equipment will be recording all conversations.
5. Begin by having a general conversation with the young person and determine his/her level of understanding and ability to communicate. Questions might include:
   - What grade are you in?
   - What school do you attend?
   - Do you have any learning disabilities?
   - How is your health?
   - Have you been arrested before?
   - Have you ever given a statement to a police officer before?
6. Review the YCJA Statement Form with the "young person" factoring in what you have learned about his/her abilities. Consider having the "young person" re-phrase what you have advised him/her so you are sure that he/she understands what you have said.
7. Have the young person sign the YCJA Statement Form.

Youth Court Record vs. Police Records

A record of proceedings under the *Youth Criminal Justice Act* can be kept by both the courts and the police.

The police can keep the following records:

1. A record of any offence alleged to have been committed by a young person, and
2. A record of any extrajudicial measure used to deal with a young person.

Youth records are kept as follows:

1. **Canadian Police Information Centre (CPIC):** the only national offender database which records data from within the formal justice system.
2. **Justin:** a provincial (BC) offender database which records data from within the formal provincial justice system.
3. **Prime:** a national offender database which records data from police contact.

The YCJA has strict control over the keeping and use of information pertaining to a young person and has set strict rules in an effort to ensure that the privacy of a young person is protected, while at the same time balancing the need for access to information to ensure an effective and efficient youth justice system. There is a general prohibition for anyone to access records kept. The exceptions to this rule are set out in s. 119 YCJA and include, but are not limited the Attorney General and any peace officer for law enforcement purposes. There are also rules relating to the length of time that access is permitted – generally the more serious the offence the longer the period of access. Once the access period has expired the Youth Court record is sealed. There are limited circumstances in which information may be accessed even after the record is sealed and are set out in the Act.
Prime records remain visible to the police even after the offender becomes an adult. There are, however, restrictions on the use of this information. For reference, Section 119 (YCJA) is in Appendix A.

Disclosure of Information Regarding a Young Person

Although records of a young person are protected, s. 125 (YCJA) indicates some situations when disclosure may be applicable and the means in which this is accomplished. Namely, the disclosure by peace officer during investigation whereby in s. 125(1) “A peace officer may disclose to any person any information in a record kept under section 114 (court records) or 115 (police records) that it is necessary to disclose in the conduct of the investigation of an offence.”

Further, in reference to disclosure of information to those person(s) listed in s. 125(6) “The provincial director, a youth worker, the Attorney General, a peace officer or any other person engaged in the provision of services to young persons may disclose to any professional or other person engaged in the supervision or care of a young person — including a representative of any school board or school or any other educational or training institution — any information contained in a record kept under sections 114 to 116 if the disclosure is necessary

- (*a*) to ensure compliance by the young person with an authorization under section 91 or an order of the youth justice court;
- (*b*) to ensure the safety of staff, students or other persons; or
- (*c*) to facilitate the rehabilitation of the young person.

Note: The entire Part 6 YCJA is available in Appendix A for reference purposes.

Investigative Guidelines

There is a misconception surrounding digital forensic evidence that there is a powerful program that will search an entire computer device and cross reference any data to police databases. Similarly people assume that there is a “magic” website that can find everything there is to know about a suspect's digital footprint. Unfortunately, there are no such tools that exist. The investigating officer should print the evidence, ask around and investigate the information they have access to first. The process for data collection includes the following:

1. Contact the service provider (for example, Facebook) and ask for a preservation order. They then have 90 days to get to it and in the meantime you can continue with your investigation. Present printed copies of the online evidence and interview witnesses. Ask some of the following questions: "Do you recognize this profile?", "Whose account is this?", "Have you ever communicated with _X_ on this profile/application?"

2. Identify material based on witnesses and present that “X” number of users have confirmed that this is the same profile. Throughout an investigation, especially in its early stages, frontline officers need to remain diligent in their articulation of what is happening at each stage. For example when conducting a search of a phone, articulate the reasoning and the judicial authority to search that device.

3. When evaluating initial digital evidence that you seize, pay particular attention to the small details within a video or a photograph. Is there evidence to support criminality in the photo/video? Can you link the evidence to the offender? Is the photo a stock image? With “cry for help” type self-harm pictures there is a trend toward youth reposting stock images found on the Internet such as cutting of the wrists. Similarly, there are cases of uploaded legitimate images depicting young people self-harming.

**** Note: it is important to follow the new test for searching cell phones and digital content (as per R. v. Fearon, 2014) (pg. 26 in this manual), especially relating to documenting the process and sequential steps by which the law enforcement officer searched the device/social media platform for evidence.**

Exigent Circumstances

Investigating officers are permitted to search and seize evidence without a warrant in exigent circumstances. Exigent circumstances exist when there is imminent danger of loss, removal, destruction or disappearance of the evidence if the search or seizure is delayed. Exigent circumstances also exist if the seizure results from the investigator carrying out the search to save a person from life-threatening immediate danger. Investigating officers must be able to articulate why the search was conducted without a warrant and why the circumstances were exigent. Police officers must be familiar with section 487 of the Criminal Code and conduct their investigations within this context.

This has been codified in s. 487.11 (when a warrant not necessary). When dealing specifically with searching a residence without a warrant, exigent circumstances have also been defined/codified under s. 529.3 (1)/ (2). There are a number of definitions for exigent circumstance and when it is appropriate for a residence, drug related or standard search. The general definition of exigent circumstances is if there is potential of imminent bodily harm or death to a person, or imminent loss or destruction of evidence, police can rely on exigent circumstances. In addition, police can rely on their common law duties, such as duty to protect life (i.e. entering a residence without a warrant after a 911 call and screams heard).

Exigent circumstances may exist when assessing an online threat or dangerous situation. Investigating officers must decide if an imminent threat exists. An example of an online threat where the police would utilize exigent circumstances may be a Facebook photo with someone showing a gun and threats to use it that day. When one compares the language and specificity of the first example to a case where an ask.fm posting states that “someone will shoot someone two weeks from” the posted date, a police officer would have a difficult time articulating to a judge how there existed exigent circumstances and police had no time to seek a warrant. If there is an imminent threat that would preclude the police from applying for/receiving a warrant due to urgency/imminent threat, then they may rely on exigent circumstances, contact Facebook (in this case), articulate why the circumstances are exigent and obtain details of IP of sender, etc.

These cases would be the same for intimidation and counselling suicide for instance, it would just be dependent on time and urgency. Unless there are exigent circumstances, warrants are needed to investigate the content of a device/computer - i.e. do not search or seize it without a warrant. The

courts are more likely to challenge the validity of the warrant over the digital evidence, so following warrant procedure is critical.

When communicating with third parties in a time sensitive investigation (Internet service providers or social media platforms), investigating officers must be able to explain the urgency of their requests and the seriousness of the investigation. This can be achieved using specific language in attempts to convey the urgency of the situation. For example, in a counselling suicide case if you are able to assign a probability or higher likelihood for this person to commit suicide based on the negative content and comments promoting completion (e.g. "Just hurry up and do it, we all F@$#ing hate you") posted online, your response time will likely be expedited.

In cyberbullying cases, it may be necessary for police officers to preserve and access the subscriber data that is retained by social media service providers. Challenges that often arise usually surround the jurisdiction of where the company is based. If the companies are based out of United States, this presents a jurisdictional challenge that may sometimes require a Mutual Legal Assistance Treaty. The following judicial authorization orders are used in assisting investigations that have a cyber component and allow Canadian authorities to preserve and produce information that is held by social media companies.

Preservation Orders

Police can obtain preservation orders to get private companies to preserve and retain data that relate to an investigation. Most companies will, when ordered, preserve data for 30 to 90 days. During this time authorities are expected to collect court issued documents that authorize the disclosure of preserved information to public agencies. Preservation orders can be submitted without court documentation. Canadian digital forensics investigators are trained to immediately issue preservation orders to social networking companies at the beginning of their investigations, if they anticipate that data might be needed to aid in an investigation. While authorities routinely issue preservation orders, these orders are not always followed up with the production orders needed to receive preserved information.[6]

Production Orders

Production orders compel private companies to deliver or make available information to authorities. Canadian production orders involve judicial oversight/authorization and can only be sought and issued by authorities. Currently, production orders are issued on a provincial basis in Canada, and are therefore authorized by provincially based judicial authorities (judges, justice of the peace). Even though judicial assent is required, they are considered less intrusive than search warrants as they do not let law enforcement officials enter and search the premises of the third party - yet their result is effectively the same. The CATSMI project research[3] found that many social networking companies

[6] Jurisdictions and Legal Strategies. The Canadian Access to Social Media Information Project. Office of the Privacy Commissioner of Canada. Found at: http://www.catsmi.ca/authorities/jurisdictions-and-legal-strategies

will disclose basic subscriber information when presented with a Canadian production order. With production orders, Canadian authorities tend to receive IP logs, mobile device or location information (if it is attached to the account), account username, as well as information about the Internet service provider (e.g. Rogers, Bell, Teksavvy) used to access the account. Investigators will typically then file another production order with the ISP that was used to access the account to get basic subscriber information (e.g. billing information, mailing address, Internet Protocol address(es) assigned to the subscriber).

Mutual Legal Assistance Treaty (MLAT)

A Mutual Legal Assistance Treaty (MLAT) facilitates cross-border (international) policing actions. In essence, MLATs are treaties between different countries that outline how they will help one another during investigations where two, or more, legal jurisdictions are involved. The MLATs that Canadian authorities use to compel information from American social networking companies typically ask American law enforcement officials to get a local court order and serve it on the company that holds the sought after data. Canadian authorities will immediately turn to an MLAT if they are investigating a serious crime (e.g. homicide). MLATs can take a long time to process, however, and so it typically takes Canadian authorities a minimum of six to eight months to receive data. Because MLATs require significant amount of bureaucratic work and can be slow to return data to authorities, these treaties are sometimes shunned in favour of open source intelligence and evidence gathering techniques.[5]

All open source data that can be gathered on the Internet or through non-login social media applications is admissible, but evidence must prove that the accused was the individual who pressed send. The digital evidence helps prove where the information came from but does not necessarily identify the computer/device user as the accused. It is easy to see what is on a device but proving who is behind the device is the key. That being said, we also acknowledge that current devices and social media are always online and logged into by their primary user. In order to prove the elements of the offence, the evidence must prove who had care and control of the computer/device used to commit the offence.

With a home computer, you have to establish that the accused had care and control of the computer at the time of the offence. Questions you might ask could include: who lives in the residence, who had access to the computer, who was at home during the time of the offence (i.e. time bracketing). At the end of the day you can't put a cellphone in jail, you need to be able to link the content to an offender. Remember that a digital evidence investigation is no different than any other - who is the victim, who is the accused, what occurred, and where can you look for further information or evidence?

A caution for investigators in using open source information and resources - what is the level of reliability for your source information, and will you be relying on it for future search warrants or orders?

Securing Evidence Case Scenario:

Potential Case:
You have a piece of digital evidence (Facebook wall post, Instagram photo with criminality, screen-shot Snapchat photo, ask.fm post with specificity around counselling suicide) - How do you go about securing the next step - Who posted/sent it?

Possible Response:
When a police officer becomes aware of digital evidence, the first concern is to secure the evidence at hand. The first step in preservation would be to screenshot or take a photograph of the digital evidence in order to time stamp it, with a URL if possible and have a permanent record of it. It would be important to interview the person who brought it to your attention in the hopes of receiving more information with regards to who else is involved. Hopefully you will be told who is responsible for the photo or content and who (if not the same person) is responsible for the posting/sharing of it. From then, you could interview any other witnesses and potentially do a warned statement of the accused. If more information is needed from the service provider, submit a preservation order to the platform and continue with investigation. Follow up with production order. Should you be able to obtain sufficient evidence from the interviews, you could obtain a search warrant to seize the computers, phones, iPods, and any other electronics that might be implicated. Any electronics seized could then be turned over to tech crimes for analysis. While this is occurring it is possible to present Crown with a bare bones file and ask for a no contact order with the victim and witnesses and a no possess/use cell phone or electronic device until the trial.

Preserving Evidence:

Foil envelopes (Mylar Evidence Bags) and Radio Frequency (RF) bags are still currently being used to preserve device evidence and the suggestion is to double bag the foil envelope. The current practice by forensics officers is to pull out the SIM card and/or battery and utilize small paint cans with lids to enclose the cell phones during storage to prevent any remote swipes of information and data. Airplane Mode works as a temporary solution. Do not turn airplane mode off, or reinsert the SIM card or battery as this could allow a remote swipe to take place.

Remember, tech crime units were created in order to deal with child pornography issues. It is important to note that they have evolved and redirected their focus to technological components of serious prioritized crimes starting with homicide, terrorism, serious violent offences, gang activity, and then child exploitation. As a result of such demand for service, current timelines for the return of a technological forensic report is 18 months. However, there has been a shift towards training more semi-technical experts to help reduce the demand on the tech crimes unit and provide support, information, and counsel to police on how to proceed in these cases. Under the RCMP's Integrated Technological Crime Unit, there exists a Digital Investigators of Computer Exhibits (DICE) team who are field triage subject area experts on technology as it relates to police investigations. RCMP members can find more information on the field triage programs (DICE and DMFT) at http://infoweb.rcmp-grc.gc.ca/edivision/branches/crim_ops/policing_support/tech_crime/FieldTriagePrograms-eng.htm

If and when an officer has to take the stand in court and present open-source social media evidence, an effective practice for describing the admission of social media evidence is to present it from a user-interface perspective. With Facebook for example, treat it as a regular service that has become commonplace. Using a user-interface perspective allows you to avoid trying to explain the inner workings of Facebook's back-end database and computer science. If you start getting too specific in your explanation, the defence will attempt to poke holes in your testimony by attempting to validate your knowledge of Facebook. If user content is received back officially from a social media platform (Facebook, Instagram, Twitter), this content is usually self-authenticating in itself.

If the police have a suspect and are considering charges, a decision, based on multiple factors, must be made as to whether to issue a PTA or when to arrest and release on bail. When there are concerns about an offender's behavioural escalation, police need to determine if it is in the best interest of the case to put that person on a PTA (Promise to Appear) vs. getting an arrest warrant and having that person released on bail terms. It is important to know that there are more protective terms available on a Bail Order vs. PTA (e.g. we couldn't ban use of computer or mobile device on a PTA but we could on a Bail Order.)

Guidelines for Prosecution and Working Together

When working with Crown Counsel, it is important to understand that jurisdiction can sometimes provide challenges or barriers depending on the resources available. In some areas, there are dedicated Youth Courts and Crown to work on youth files. In many areas, this is not an option and therefore those prosecutors may not have the same level of experience or understanding of youth trends, issues and behaviours.

Crown Counsel assesses charges by applying the charge approval standard. In order for charges to be approved, there must be a substantial likelihood of conviction and the prosecution must be in the public interest. Crown counsel weigh these two factors in deciding whether or not to approve charges.

Crown needs to decide what the appropriate response will be. In order to do that, they need to look at *both* the considerations for the *offence* as it occurred and the *offender* alleged to have committed that offence.

- When we look at the Offender, we consider some of the following:
  - What is their legal history (police contacts, has EJM been used before, etc.)
  - What is their family situation?
  - Are there any psychological issues/mental health concerns?
  - Do they demonstrate remorse for their actions?
  - What was their relationship to the victim?
  - What was the context of the incident?
  - What was the effect on others? For example, bystanders.

One of the main concerns that arose in discussion with prosecutors was around the use of restorative justice and a concern regarding its appropriateness in dealing with cyberbullying. Crown's decision to proceed with charges or refer the file to restorative justice programs varies across BC. It is understood that this is case-by-case and that the public interest will vary amongst jurisdictions, which impacts on providing a consistent response to dealing with cyberbullying behaviours that are, or border on, criminal offences.

Guidelines for Probation

Challenges:

Youth Probation has some concerns regarding appropriate means of responding to the cases/clients who come to their attention. Questions remain regarding how to monitor and enforce court orders that an offender stay off of the Internet/computer and how to work with those on a caseload to educate and prevent further incidents.

According to subject matter resources, it is important to understand the trends of young people and their online behaviour. The more that is known, the better equipped youth probation is to respond in an appropriate way. This is almost parallel to the parental role around setting expectations and educating clients around the risks/dangers of their online behaviour. It is understood that when working with youth, success is often largely dependent on the relationships built within. The response in dealing with young people under supervision for cyber-based behaviour won't be vastly different than other cases. There is not a simplistic answer, but the aim of this resource is to work with young people in a preventative way that hopefully precludes the need to respond after-the-fact on a regular basis.

Beyond that, when responding to an order that may include a "no-go" to a computer or device, similarly to police, you can utilize open source gathering techniques (known usernames on the major social media platforms, using the online friends of this person to monitor interactions). In today's technological age it can be very difficult to track if someone is using the Internet given the available resources (IP blocking, Internet cafes, private networks). Again, fall back to traditional investigative techniques where you physically catch this person using a device or computer. Whether it is physical observations or video footage of the offender using a public library computer or Starbucks Wi-Fi connection. Collateral contacts with parents/caregivers are also a primary means of determining compliance with these types of conditions.

Guideline for Victim Support Workers

How do we Best Support Victims of Cyberbullying?

When we are looking at means of supporting those who have been victimized online, we need to be mindful of the aforementioned challenges and emotional volatility of these occurrences. Similarly to other crimes, victims of cyberbullying are often in need of information and emotional support. However, there are unique factors present in cyberbullying cases that make them different from other instances of victimization. Some of those unique factors are outlined on page 9 of this document and include:

- 24/7 availability of the Internet;
- Possible anonymity of the perpetrator; and
- Scope of the audience and permanence of the victimization

Because of the unique nature of cyberbullying, a unique approach may be needed to support victims more effectively. Some additional things that are important in providing support may include:

- Understanding the victim's role in the incident;
- Recognizing the emotional responses;
- Working effectively with support networks; and
- Providing support and education moving forward.

Understanding the Victim's Role in the Incident

Without victim blaming or shaming, it is important to be aware of the role that the victim may have played in the incident, and how their role could be affecting their reaction to it. Depending on their role in the incident, victims can feel shame, humiliation, resentment, self-blame, guilt and anger. It is important to be able to understand their role, and also to convey a message to the victim that it is not their fault that they have victimized.

Recognizing and Responding to the Emotional Responses

As with other offences, victims can produce physical responses to cyberbullying. Research has proven that there are many different physiological impacts. Headaches, stomach issues, skin reactions, sleep disturbances, eating disorders, mental health issues including depression, self-harming behaviours or suicide attempts are all possible outcomes for someone who has been traumatized by severe online attacks.

As a victim support worker, it would be important to identify this emotional response to cyberbullying behaviours, and be able to respond and seek additional support for the victim. Talking about suicide and self-injury can be uncomfortable. As support staff, it is important to know your own limits and comfort zones and respect them.

Self-harm is thought to be DIRECTLY linked with suicide but this isn't the case. The two will often get lumped together because both are reflections of emotional pain. Generally people who self-harm do not wish to kill themselves; whereas suicide is a way of ending life.

The most significant difference between suicide and self-harm is intent. A suicidal person sees no way out and wants to end his or her life. People who are contemplating suicide are experiencing life stressors, risk enhancers and likely depression in which they don't have an escape. Suicide is their attempt to escape pain and suffering, and not burdening loved ones any longer. Suicidal acts usually come from a place of hopelessness, depression and worthlessness. The bottom line is someone who is suicidal and someone who is engaging in self-harm behaviours is very different.

Individuals who engage in self-harm find the behaviour as a way of coping with their life. It is imperative that professionals recognize the difference between the behaviours so successful intervention and prevention plans can be put in to place.

Suicide	Self-injury
Intent to end life	Intent to feel relief from intense feelings or numbness
Lethal means used	Non-lethal means used
Often a single event	Repeated behavior
No sense of relief after attempt	Immediate sense of relief after self-injuring
Feeling hopeless and helpless	A sense of having some control over emotions
In response to feeling of inescapable and unending pain	In response to feeling overwhelmed by emotions or feeling numb

Warning Signs of Potential Self Harming Behaviours:

- Long sleeves in warm weather/refusing to show arms or other body parts
- Frequent injuries with weak explanations
- Tools (unbent paperclips, razors, lighters, knives, shards of glass, etc.)
- Risk-taking behaviors
- Lack of healthy coping skills

What to Do:

- Ask about suicide
- Ask to see cuts (if you're comfortable and they're willing) – how many, how deep, how are they healing, are they infected?
- Find out about triggers – what feelings or situations make them want to self-injure?
- What brings their risk/urge to self-injure down?
- What do they do to cope when they can't injure?

Self-harm is a way of dealing with feelings and difficult situations. If they're going to stop, they need to have alternative ways of coping in place so they can respond differently when they start to feel like cutting or harming themselves.

Self-Harm Alternatives (coping skills)

- Angry – run, punching bag, rip up old phonebooks/newspapers
- Sad – hot bath, read, listen to music, yoga, self-care (hair, nails, etc.), sleep/nap, eat
- Focus – paint nails, play videogames, do something that takes concentration
- Blood – red marker, red food coloring, paint
- Scabs – Get a henna kit

Working Effectively with Support Networks

Experience has indicated that bullying behaviours tend to subside somewhat when there isn't retaliation from the victim or their supporters. It is important to be clear with both the victim and their supporters that retaliation can often escalate a bullying situation further.

Victim service professionals also note that the role of the family members who are "supporting" the target can also be problematic in some situations. Parents of young victims are understandably protective of their children and want to do what they can to help. Often times, they also can make things more complex when they over-protect long after the incident. When a young victim wants to move forward and try to forget about a situation, parents may stand in the way as they, themselves seek "justice" against the wishes of their child. Supporting a victim can also mean ensuring that their support networks understand the impact that they may be having on the victim's recovery from the incident.

Providing Support and Education Moving Forward

The best support for a victim is dependent on the unique needs of that particular victim. Young victims can often be assisted through emotional support and counselling. Depending on the situation, education to prevent future occurrences of bullying could also be helpful. This could include discussing use of online sites and privacy issues that may arise when creating an online network.

Appendix C contains further information and resources that could assist in supporting victims of cyberbullying.

See Appendix F for Reporting Form for Privacy Commissioner

Appendix A: Key Knowledge Areas of the YCJA

YCJA Information:

Below are the pertinent sections of the YCJA which will provide a quick reference for some basic information within the Act.

DECLARATION OF PRINCIPLE

Policy for Canada with Respect to Young Persons

3. (1) The following principles apply in this Act:

- (*a*) the youth criminal justice system **is intended to protect the public** by:
    - (i) holding young persons accountable through measures that are proportionate to the seriousness of the offence and the degree of responsibility of the young person;
    - (ii) promoting the rehabilitation and reintegration of young persons who have committed offences, and
    - (iii) supporting the prevention of crime by referring young persons to programs or agencies in the community to address the circumstances underlying their offending behaviour.
- (*b*) the criminal justice system for young persons **must be separate from that of adults, must be based on the principle of diminished moral blameworthiness or culpability and must emphasize the following:**
    - (i) rehabilitation and reintegration;
    - (ii) fair and proportionate accountability that is consistent with the greater dependency of young persons and their reduced level of maturity;
    - (iii) enhanced procedural protection to ensure that young persons are treated fairly and that their rights, including their right to privacy, are protected;
    - (iv) timely intervention that reinforces the link between the offending behaviour and its consequences, and
    - (v) the promptness and speed with which persons responsible for enforcing this Act must act, given young persons perception of time.
- (*c*) **within the limits of fair and proportionate accountability, the measures taken against young persons who commit offences should:**
    - (i) reinforce respect for societal values;
    - (ii) encourage the repair of harm done to victims and the community;

- (iii) be meaningful for the individual young person given his or her needs and level of development and, where appropriate, involve the parents, the extended family, the community and social or other agencies in the young person's rehabilitation and reintegration, and
- (iv) respect gender, ethnic, cultural and linguistic differences and respond to the needs of aboriginal young persons and of young persons with special requirements; and

- (*d*) **special considerations apply** in respect of proceedings against young persons and, in particular,
  - (i) young persons have rights and freedoms in their own right, such as a right to be heard in the course of, and to participate in the processes, other than the decision to prosecute, that lead to decisions that affect them, and young persons have special guarantees of their rights and freedoms;
  - (ii) victims should be treated with courtesy, compassion and respect for their dignity and privacy and should suffer the minimum degree of inconvenience as a result of their involvement with the youth criminal justice system;
  - (iii) victims should be provided with information about the proceedings and given an opportunity to participate and be heard, and
  - (iv) parents should be informed of measures or proceedings involving their children and encouraged to support them in addressing their offending behaviour.

PART 1
EXTRAJUDICIAL MEASURES
Principles and Objectives

Declaration of Principles
4. The following principles apply in this part in addition to the principles set out in section 3:
- (*a*) extrajudicial measures are often the most appropriate and effective way to address youth crime;
- (*b*) extrajudicial measures allow for effective and timely interventions focused on correcting offending behaviour;
- (*c*) extrajudicial measures are presumed to be adequate to hold a young person accountable for his or her offending behaviour if the young person has committed a non-violent offence and has not previously been found guilty of an offence; and
- (*d*) extrajudicial measures should be used if they are adequate to hold a young person accountable for his or her offending behaviour and, if the use of extrajudicial measures is consistent with the principles set out in this section, nothing in this Act precludes their use in respect of a young person who:
  - (i) has previously been dealt with by the use of extrajudicial measures, or
  - (ii) has previously been found guilty of an offence.

Objectives

5. Extrajudicial measures should be designed to:

- (*a*) provide an effective and timely response to offending behaviour outside the bounds of judicial measures;
- (*b*) encourage young persons to acknowledge and repair the harm caused to the victim and the community;
- (*c*) encourage families of young persons, including extended families where appropriate, and the community, to become involved in the design and implementation of those measures;
- (*d*) provide an opportunity for victims to participate in decisions related to the measures selected and to receive reparation; and
- (*e*) respect the rights and freedoms of young persons and be proportionate to the seriousness of the offence.

Warnings, Cautions and Referrals

6. (1) A police officer shall, before starting judicial proceedings or taking any other measures under this Act against a young person alleged to have committed an offence, consider whether it would be sufficient, having regard to the principles set out in section 4, to take no further action, warn the young person, administer a caution, if a program has been established under section 7, or, with the consent of the young person, refer the young person to a program or agency in the community that may assist the young person not to commit offences.

Saving

(2) The failure of a police officer to consider the options set out in subsection (1) does not invalidate any subsequent charges against the young person for the offence.

Police Cautions

7. The Attorney General, or any other minister designated by the lieutenant governor of a province, may establish a program authorizing the police to administer cautions to young persons instead of starting judicial proceedings under this Act.

Crown Cautions

8. The Attorney General may establish a program authorizing prosecutors to administer cautions to young persons instead of starting or continuing judicial proceedings under this Act.

Evidence of Measures is Inadmissible

9. Evidence that a young person has received a warning, caution or referral mentioned in section 6, 7 or 8 or that a police officer has taken no further action in respect of an offence, and evidence of the offence, is inadmissible for the purpose of proving prior offending behaviour in any proceedings before a youth justice court in respect of the young person.

Extrajudicial Sanctions

- **10.** (1) An extrajudicial sanction may be used to deal with a young person alleged to have committed an offence only if the young person cannot be adequately dealt with by a warning, caution or referral mentioned in section 6, 7 or 8 because of the seriousness of the offence, the nature and number of previous offences committed by the young person or any other aggravating circumstances.

Conditions
(2) An extrajudicial sanction may be used only if:

- (*a*) it is part of a program of sanctions that may be authorized by the Attorney General or authorized by a person, or a member of a class of persons, designated by the lieutenant governor in council of the province;
- (*b*) the person who is considering whether to use the extrajudicial sanction is satisfied that it would be appropriate, having regard to the needs of the young person and the interests of society;
- (*c*) the young person, having been informed of the extrajudicial sanction, fully and freely consents to be subject to it;
- (*d*) the young person has, before consenting to be subject to the extrajudicial sanction, been advised of his or her right to be represented by counsel and been given a reasonable opportunity to consult with counsel;
- (*e*) the young person accepts responsibility for the act or omission that forms the basis of the offence that he or she is alleged to have committed;
- (*f*) there is, in the opinion of the Attorney General, sufficient evidence to proceed with the prosecution of the offence; and
- (*g*) the prosecution of the offence is not in any way barred at law.

Restriction on Use
(3) An extrajudicial sanction may not be used in respect of a young person who

- (*a*) denies participation or involvement in the commission of the offence; or
- (*b*) expresses the wish to have the charge dealt with by a youth justice court.

Admissions not Admissible in Evidence
(4) Any admission, confession or statement accepting responsibility for a given act or omission that is made by a young person as a condition of being dealt with by extrajudicial measures is inadmissible in evidence against any young person in civil or criminal proceedings.

No Bar to Judicial Proceedings
(5) The use of an extrajudicial sanction in respect of a young person alleged to have committed an offence is not a bar to judicial proceedings under this Act, but if a charge is laid against the young person in respect of the offence,

- (*a*) the youth justice court shall dismiss the charge if it is satisfied on a balance of probabilities that the young person has totally complied with the terms and conditions of the extrajudicial sanction; and
- (*b*) the youth justice court may dismiss the charge if it is satisfied on a balance of probabilities that the young person has partially complied with the terms and conditions of the extrajudicial sanction and if, in the opinion of the court, prosecution of the charge would be unfair having regard to the circumstances and the young person's performance with respect to the extrajudicial sanction.

Laying of Information, etc.
(6) Subject to subsection (5) and section 24 (private prosecutions only with consent of Attorney General), nothing in this section shall be construed as preventing any person from laying an information or indictment, obtaining the issue or confirmation of any process or proceeding with the prosecution of any offence in accordance with law.

Notice to Parent
11. If a young person is dealt with by an extrajudicial sanction, the person who administers the program under which the sanction is used shall inform a parent of the young person of the sanction.

Victim's Right to Information
12. If a young person is dealt with by an extrajudicial sanction, a police officer, the Attorney General, the provincial director or any organization established by a province to provide assistance to victims shall, on request, inform the victim of the identity of the young person and how the offence has been dealt with.

PART 4
SENTENCING
Purpose and Principles

Purpose

- **38.** (1) The purpose of sentencing under section 42 (youth sentences) is to hold a young person accountable for an offence through the imposition of just sanctions that have meaningful consequences for the young person and that promote his or her rehabilitation and reintegration into society, thereby contributing to the long-term protection of the public.

Sentencing Principles
(2) A youth justice court that imposes a youth sentence on a young person shall determine the sentence in accordance with the principles set out in section 3 and the following principles:

- (*a*) the sentence must not result in a punishment that is greater than the punishment that would be appropriate for an adult who has been convicted of the same offence committed in similar circumstances;
- (*b*) the sentence must be similar to the sentences imposed in the region on similar young persons found guilty of the same offence committed in similar circumstances;
- (*c*) the sentence must be proportionate to the seriousness of the offence and the degree of responsibility of the young person for that offence;
- (*d*) all available sanctions other than custody that are reasonable in the circumstances should be considered for all young persons, with particular attention to the circumstances of aboriginal young persons;
- (*e*) subject to paragraph (*c*), the sentence must:
  - (i) be the least restrictive sentence that is capable of achieving the purpose set out in subsection (1),
  - (ii) be the one that is most likely to rehabilitate the young person and reintegrate him or her into society, and
  - (iii) promote a sense of responsibility in the young person, and an acknowledgement of the harm done to victims and the community; and
- (*f*) subject to paragraph (*c*), the sentence may have the following objectives:
  - (i) to denounce unlawful conduct, and
  - (ii) to deter the young person from committing offences.

Factors to be Considered
(3) In determining a youth sentence, the youth justice court shall take into account:

- (*a*) the degree of participation by the young person in the commission of the offence;
- (*b*) the harm done to victims and whether it was intentional or reasonably foreseeable;
- (*c*) any reparation made by the young person to the victim or the community;
- (*d*) the time spent in detention by the young person as a result of the offence;
- (*e*) the previous findings of guilt of the young person; and
- (*f*) any other aggravating and mitigating circumstances related to the young person or the offence that are relevant to the purpose and principles set out in this section.

Youth Sentences

Recommendation of Conference

41. When a youth justice court finds a young person guilty of an offence, the court may convene or cause to be convened a conference under section 19 for recommendations to the court on an appropriate youth sentence.

Considerations as to Youth Sentence

- **42.** (1) A youth justice court shall, before imposing a youth sentence, consider any recommendations submitted under section 41, any pre-sentence report, any representations made by the parties to the proceedings or their counsel or agents and by the parents of the young person, and any other relevant information before the court.

Youth Sentence

(2) When a youth justice court finds a young person guilty of an offence and is imposing a youth sentence, the court shall, subject to this section, impose any one of the following sanctions or any number of them that are not inconsistent with each other and, if the offence is first degree murder or second degree murder within the meaning of section 231 of the *Criminal Code*, the court shall impose a sanction set out in paragraph (*q*) or subparagraph (*r*)(ii) or (iii) and may impose any other of the sanctions set out in this subsection that the court considers appropriate:

- (*a*) reprimand the young person;
- (*b*) by order direct that the young person be discharged absolutely, if the court considers it to be in the best interests of the young person and not contrary to the public interest;
- (*c*) by order direct that the young person be discharged on any conditions that the court considers appropriate and may require the young person to report to and be supervised by the provincial director;
- (*d*) impose on the young person a fine not exceeding $1,000 to be paid at the time and on the terms that the court may fix;
- (*e*) order the young person to pay to any other person at the times and on the terms that the court may fix an amount by way of compensation for loss of or damage to property or for loss of income or support, or an amount for, in the Province of Quebec, pre-trial pecuniary loss or, in any other province, special damages, for personal injury arising from the commission of the offence if the value is readily ascertainable, but no order shall be made for other damages in the Province of Quebec or for general damages in any other province;
- (*f*) order the young person to make restitution to any other person of any property obtained by the young person as a result of the commission of the offence within the time that the court may fix, if the property is owned by the other person or was, at the time of the offence, in his or her lawful possession;
- (*g*) if property obtained as a result of the commission of the offence has been sold to an innocent purchaser, where restitution of the property to its owner or any other person has been made or ordered, order the young person to pay the purchaser, at the time and on the terms that the court may fix, an amount not exceeding the amount paid by the purchaser for the property;
- (*h*) subject to section 54, order the young person to compensate any person in kind or by way of personal services at the time and on the terms that the court may fix for any loss, damage or injury suffered by that person in respect of which an order may be made under paragraph (*e*) or (*g*);

- (*i*) subject to section 54, order the young person to perform a community service at the time and on the terms that the court may fix, and to report to and be supervised by the provincial director or a person designated by the youth justice court;
- (*j*) subject to section 51 (mandatory prohibition order), make any order of prohibition, seizure or forfeiture that may be imposed under any Act of Parliament or any regulation made under it if an accused is found guilty or convicted of that offence, other than an order under section 161 of the *Criminal Code*;
- (*k*) place the young person on probation in accordance with sections 55 and 56 (conditions and other matters related to probation orders) for a specified period not exceeding two years;
- (*l*) subject to subsection (3) (agreement of provincial director), order the young person into an intensive support and supervision program approved by the provincial director;
- (*m*) subject to subsection (3) (agreement of provincial director) and section 54, order the young person to attend a non-residential program approved by the provincial director, at the times and on the terms that the court may fix, for a maximum of two hundred and forty hours, over a period not exceeding six months;
- (*n*) make a custody and supervision order with respect to the young person, ordering that a period be served in custody and that a second period — which is one half as long as the first — be served, subject to sections 97 (conditions to be included) and 98 (continuation of custody), under supervision in the community subject to conditions, the total of the periods not to exceed two years from the date of the coming into force of the order or, if the young person is found guilty of an offence for which the punishment provided by the *Criminal Code* or any other Act of Parliament is imprisonment for life, three years from the date of coming into force of the order;
- (*o*) in the case of an offence set out in section 239 (attempt to commit murder), 232, 234 or 236 (manslaughter) or 273 (aggravated sexual assault) of the *Criminal Code*, make a custody and supervision order in respect of the young person for a specified period not exceeding three years from the date of committal that orders the young person to be committed into a continuous period of custody for the first portion of the sentence and, subject to subsection 104(1) (continuation of custody), to serve the remainder of the sentence under conditional supervision in the community in accordance with section 105;
- (*p*) subject to subsection (5), make a deferred custody and supervision order that is for a specified period not exceeding six months, subject to the conditions set out in subsection 105(2), and to any conditions set out in subsection 105(3) that the court considers appropriate;
- (*q*) order the young person to serve a sentence not to exceed:
    - (i) in the case of first degree murder, ten years comprised of
        - (A) a committal to custody, to be served continuously, for a period that must not, subject to subsection 104(1) (continuation of custody), exceed six years from the date of committal, and
        - (B) a placement under conditional supervision to be served in the community in accordance with section 105, and
    - (ii) in the case of second degree murder, seven years comprised of
        - (A) a committal to custody, to be served continuously, for a period that must not, subject to subsection 104(1) (continuation of custody), exceed four years from the date of committal, and

        - (B) a placement under conditional supervision to be served in the community in accordance with section 105;
    - (*r*) subject to subsection (7), make an intensive rehabilitative custody and supervision order in respect of the young person
        - (i) that is for a specified period that must not exceed:
            - (A) two years from the date of committal, or
            - (B) if the young person is found guilty of an offence for which the punishment provided by the *Criminal Code* or any other Act of Parliament is imprisonment for life, three years from the date of committal, and that orders the young person to be committed into a continuous period of intensive rehabilitative custody for the first portion of the sentence and, subject to subsection 104(1) (continuation of custody), to serve the remainder under conditional supervision in the community in accordance with section 105,
        - (ii) that is for a specified period that must not exceed, in the case of first degree murder, ten years from the date of committal, comprising
            - (A) a committal to intensive rehabilitative custody, to be served continuously, for a period that must not exceed six years from the date of committal, and
            - (B) subject to subsection 104(1) (continuation of custody), a placement under conditional supervision to be served in the community in accordance with section 105, and
        - (iii) that is for a specified period that must not exceed, in the case of second degree murder, seven years from the date of committal, comprising
            - (A) a committal to intensive rehabilitative custody, to be served continuously, for a period that must not exceed four years from the date of committal, and
            - (B) subject to subsection 104(1) (continuation of custody), a placement under conditional supervision to be served in the community in accordance with section 105; and
    - (*s*) impose on the young person any other reasonable and ancillary conditions that the court considers advisable and in the best interests of the young person and the public.

PART 6
PUBLICATION, RECORDS AND INFORMATION
Protection of Privacy of Young Persons

Identity of Offender not to be Published

- **110.** (1) Subject to this section, no person shall publish the name of a young person, or any other information related to a young person, if it would identify the young person as a young person dealt with under this Act.

Limitation
(2) Subsection (1) does not apply

- (*a*) in a case where the information relates to a young person who has received an adult sentence;
- (*b*) in a case where the information relates to a young person who has received a youth sentence for a violent offence and the youth justice court has ordered a lifting of the publication ban under subsection 75(2); and
- (*c*) in a case where the publication of information is made in the course of the administration of justice, if it is not the purpose of the publication to make the information known in the community.

Exception
(3) A young person referred to in subsection (1) may, after he or she attains the age of eighteen years, publish or cause to be published information that would identify him or her as having been dealt with under this Act or the *Young Offenders Act*, chapter Y-1 of the Revised Statutes of Canada, 1985, provided that he or she is not in custody pursuant to either Act at the time of the publication.

***Ex Parte* Application for Leave to Publish**
(4) A youth justice court judge shall, on the *ex parte* application of a peace officer, make an order permitting any person to publish information that identifies a young person as having committed or allegedly committed an indictable offence, if the judge is satisfied that:

- (*a*) there is reason to believe that the young person is a danger to others; and
- (*b*) publication of the information is necessary to assist in apprehending the young person.

Order Ceases to Have Effect
(5) An order made under subsection (4) ceases to have effect five days after it is made
.
Application for Leave to Publish
(6) The youth justice court may, on the application of a young person referred to in subsection (1), make an order permitting the young person to publish information that would identify him or her as having been dealt with under this Act or the *Young Offenders Act*, chapter Y-1 of the Revised Statutes of Canada, 1985, if the court is satisfied that the publication would not be contrary to the young person's best interests or the public interest.

- 2002, c. 1, s. 110;
- 2012, c. 1, s. 189.

Identity of Victim or Witness not to be Published

- **111.** (1) Subject to this section, no person shall publish the name of a child or young person, or any other information related to a child or a young person, if it would identify the child or young person as having been a victim of, or as having appeared as a witness in connection with, an offence committed or alleged to have been committed by a young person.

Exception
(2) Information that would serve to identify a child or young person referred to in subsection (1) as having been a victim or a witness may be published, or caused to be published, by:

- (*a*) that child or young person after he or she attains the age of eighteen years or before that age with the consent of his or her parents; or
- (*b*) the parents of that child or young person if he or she is deceased.

Application for Leave to Publish
(3) The youth justice court may, on the application of a child or a young person referred to in subsection (1), make an order permitting the child or young person to publish information that would identify him or her as having been a victim or a witness if the court is satisfied that the publication would not be contrary to his or her best interests or the public interest.

Non-application
112. Once information is published under subsection 110(3) or (6) or 111(2) or (3), subsection 110(1) (identity of offender not to be published) or 111(1) (identity of victim or witness not to be published), as the case may be, no longer applies in respect of the information.

Fingerprints and Photographs
***Identification of Criminals Act* applies:**

- **113.** (1) The *Identification of Criminals Act* applies in respect of young persons.

Limitation
(2) No fingerprint, palmprint or photograph or other measurement, process or operation referred to in the *Identification of Criminals Act* shall be taken of, or applied in respect of, a young person who is charged with having committed an offence except in the circumstances in which an adult may, under that Act, be subjected to the measurements, processes and operations.

Records That May Be Kept

Youth Justice Court, Review Board and Other Courts
114. A youth justice court, review board or any court dealing with matters arising out of proceedings under this Act may keep a record of any case that comes before it arising under this Act.

Police Records

- **115.** (1) A record relating to any offence alleged to have been committed by a young person, including the original or a copy of any fingerprints or photographs of the young person, may be kept by any police force responsible for or participating in the investigation of the offence.

Extrajudicial Measures
(1.1) The police force shall keep a record of any extrajudicial measures that they use to deal with young persons.

Police Records
(2) When a young person is charged with having committed an offence in respect of which an adult may be subjected to any measurement, process or operation referred to in the *Identification of*

Criminals Act, the police force responsible for the investigation of the offence may provide a record relating to the offence to the Royal Canadian Mounted Police. If the young person is found guilty of the offence, the police force shall provide the record.

Records Held by R.C.M.P.
(3) The Royal Canadian Mounted Police shall keep the records provided under subsection (2) in the central repository that the Commissioner of the Royal Canadian Mounted Police may, from time to time, designate for the purpose of keeping criminal history files or records of offenders or keeping records for the identification of offenders.

- 2002, c. 1, s. 115;
- 2012, c. 1, s. 190.

Government Records

- **116.** (1) A department or an agency of any government in Canada may keep records containing information obtained by the department or agency:
  - (*a*) for the purposes of an investigation of an offence alleged to have been committed by a young person;
  - (*b*) for use in proceedings against a young person under this Act;
  - (*c*) for the purpose of administering a youth sentence or an order of the youth justice court;
  - (*d*) for the purpose of considering whether to use extrajudicial measures to deal with a young person; or
  - (*e*) as a result of the use of extrajudicial measures to deal with a young person.

Other Records
(2) A person or organization may keep records containing information obtained by the person or organization:

  - (*a*) as a result of the use of extrajudicial measures to deal with a young person; or
  - (*b*) for the purpose of administering or participating in the administration of a youth sentence.

Access to Records

Exception — Adult Sentence
117. Sections 118 to 129 do not apply to records kept in respect of an offence for which an adult sentence has been imposed once the time allowed for the taking of an appeal has expired or, if an appeal is taken, all proceedings in respect of the appeal have been completed and the appeal court has upheld an adult sentence. The record shall be dealt with as a record of an adult and, for the purposes of the *Criminal Records Act*, the finding of guilt in respect of the offence for which the record is kept is deemed to be a conviction.

No Access Unless Authorized

- **118.** (1) Except as authorized or required by this Act, no person shall be given access to a record kept under sections 114 to 116, and no information contained in it may be given to any person, where to do so would identify the young person to whom it relates as a young person dealt with under this Act.

Exception for Employees
(2) No person who is employed in keeping or maintaining records referred to in subsection (1) is restricted from doing anything prohibited under subsection (1) with respect to any other person so employed.

Persons Having Access to Records

- **119.** (1) Subject to subsections (4) to (6), from the date that a record is created until the end of the applicable period set out in subsection (2), the following persons, on request, shall be given access to a record kept under section 114, and may be given access to a record kept under sections 115 and 116:
    - (*a*) the young person to whom the record relates;
    - (*b*) the young person's counsel, or any representative of that counsel;
    - (*c*) the Attorney General;
    - (*d*) the victim of the offence or alleged offence to which the record relates;
    - (*e*) the parents of the young person, during the course of any proceedings relating to the offence or alleged offence to which the record relates or during the term of any youth sentence made in respect of the offence;
    - (*f*) any adult assisting the young person under subsection 25(7), during the course of any proceedings relating to the offence or alleged offence to which the record relates or during the term of any youth sentence made in respect of the offence;
    - (*g*) any peace officer for:
        - (i) law enforcement purposes, or
        - (ii) any purpose related to the administration of the case to which the record relates, during the course of proceedings against the young person or the term of the youth sentence;
    - (*h*) a judge, court or review board, for any purpose relating to proceedings against the young person, or proceedings against the person after he or she becomes an adult, in respect of offences committed or alleged to have been committed by that person;
    - (*i*) the provincial director, or the director of the provincial correctional facility for adults or the penitentiary at which the young person is serving a sentence;
    - (*j*) a person participating in a conference or in the administration of extrajudicial measures, if required for the administration of the case to which the record relates;
    - (*k*) a person acting as ombudsman, privacy commissioner or information commissioner, whatever his or her official designation might be, who in the course of his or her duties under an Act of Parliament or the legislature of a province is investigating a complaint to which the record relates;
    - (*l*) a coroner or a person acting as a child advocate, whatever his or her official designation might be, who is acting in the course of his or her duties under an Act of Parliament or the legislature of a province;
    - (*m*) a person acting under the *Firearms Act*;
    - (*n*) a member of a department or agency of a government in Canada, or of an organization that is an agent of, or under contract with, the department or agency, who is:
        - (i) acting in the exercise of his or her duties under this Act,
        - (ii) engaged in the supervision or care of the young person, whether as a young person or an adult, or in an investigation related to the young person under an Act of the legislature of a province respecting child welfare,
        - (iii) considering an application for conditional release, or for a record suspension under the *Criminal Records Act*, made by the young person, whether as a young person or an adult,
        - (iv) administering a prohibition order made under an Act of Parliament or the legislature of a province, or

        - (v) administering a youth sentence, if the young person has been committed to custody and is serving the custody in a provincial correctional facility for adults or a penitentiary;
    - (*o*) a person, for the purpose of carrying out a criminal record check required by the Government of Canada or the government of a province or a municipality for purposes of employment or the performance of services, with or without remuneration;
    - (*p*) an employee or agent of the Government of Canada, for statistical purposes under the *Statistics Act*;
    - (*q*) an accused or his or her counsel who swears an affidavit to the effect that access to the record is necessary to make a full answer and defence;
    - (*r*) a person or a member of a class of persons designated by order of the Governor in Council, or the lieutenant governor in council of the appropriate province, for a purpose and to the extent specified in the order; and
    - (*s*) any person or member of a class of persons that a youth justice court judge considers has a valid interest in the record, to the extent directed by the judge, if the judge is satisfied that access to the record is:
        - (i) desirable in the public interest for research or statistical purposes, or
        - (ii) desirable in the interest of the proper administration of justice.

Period of Access

(2) The period of access referred to in subsection (1) is:

- (*a*) if an extrajudicial sanction is used to deal with the young person, the period ending two years after the young person consents to be subject to the sanction in accordance with paragraph 10(2)(*c*);
- (*b*) if the young person is acquitted of the offence otherwise than by reason of a verdict of not criminally responsible on account of mental disorder, the period ending two months after the expiry of the time allowed for the taking of an appeal or, if an appeal is taken, the period ending three months after all proceedings in respect of the appeal have been completed;
- (*c*) if the charge against the young person is dismissed for any reason other than acquittal, the charge is withdrawn, or the young person is found guilty of the offence and a reprimand is given, the period ending two months after the dismissal, withdrawal, or finding of guilt;
- (*d*) if the charge against the young person is stayed, with no proceedings being taken against the young person for a period of one year, at the end of that period;
- (*e*) if the young person is found guilty of the offence and the youth sentence is an absolute discharge, the period ending one year after the young person is found guilty;
- (*f*) if the young person is found guilty of the offence and the youth sentence is a conditional discharge, the period ending three years after the young person is found guilty;
- (*g*) subject to paragraphs (*i*) and (*j*) and subsection (9), if the young person is found guilty of the offence and it is a summary conviction offence, the period ending three years after the youth sentence imposed in respect of the offence has been completed;
- (*h*) subject to paragraphs (*i*) and (*j*) and subsection (9), if the young person is found guilty of the offence and it is an indictable offence, the period ending five years after the youth sentence imposed in respect of the offence has been completed;
- (*i*) subject to subsection (9), if, during the period calculated in accordance with paragraph (*g*) or (*h*), the young person is found guilty of an offence punishable on summary conviction committed when he or she was a young person, the latest of:
    - (i) the period calculated in accordance with paragraph (*g*) or (*h*), as the case may be, and

        - (ii) the period ending three years after the youth sentence imposed for that offence has been completed; and
    - (*j*) subject to subsection (9), if, during the period calculated in accordance with paragraph (*g*) or (*h*), the young person is found guilty of an indictable offence committed when he or she was a young person, the period ending five years after the sentence imposed for that indictable offence has been completed.

Prohibition Orders not Included
(3) Prohibition orders made under an Act of Parliament or the legislature of a province, including any order made under section 51, shall not be taken into account in determining any period referred to in subsection (2).

Extrajudicial Measures
(4) Access to a record kept under section 115 or 116 in respect of extrajudicial measures, other than extrajudicial sanctions, used in respect of a young person shall be given only to the following persons for the following purposes:

- (*a*) a peace officer or the Attorney General, in order to make a decision whether to again use extrajudicial measures in respect of the young person;
- (*b*) a person participating in a conference, in order to decide on the appropriate extrajudicial measure;
- (*c*) a peace officer, the Attorney General or a person participating in a conference, if access is required for the administration of the case to which the record relates; and
- (*d*) a peace officer for the purpose of investigating an offence.

Exception
(5) When a youth justice court has withheld all or part of a report from any person under subsection 34(9) or (10) (nondisclosure of medical or psychological report) or 40(7) (nondisclosure of pre-sentence report), that person shall not be given access under subsection (1) to that report or part.

Records of Assessments or Forensic DNA Analysis
(6) Access to a report made under section 34 (medical and psychological reports) or a record of the results of forensic DNA analysis of a bodily substance taken from a young person in execution of a warrant issued under section 487.05 of the *Criminal Code* may be given only under paragraphs (1)(*a*) to (*c*), (*e*) to (*h*) and (*q*) and subparagraph (1)(*s*)(ii).

Introduction into Evidence
(7) Nothing in paragraph (1)(*h*) or (*q*) authorizes the introduction into evidence of any part of a record that would not otherwise be admissible in evidence.

Disclosures for Research or Statistical Purposes
(8) When access to a record is given to a person under paragraph (1)(*p*) or subparagraph (1)(*s*)(i), the person may subsequently disclose information contained in the record, but shall not disclose the information in any form that would reasonably be expected to identify the young person to whom it relates.

Application of Usual Rules
(9) If, during the period of access to a record under any of paragraphs (2)(*g*) to (*j*), the young person is convicted of an offence committed when he or she is an adult:

- (*a*) section 82 (effect of absolute discharge or termination of youth sentence) does not apply to the young person in respect of the offence for which the record is kept under sections 114 to 116;
- (*b*) this Part no longer applies to the record and the record shall be dealt with as a record of an adult; and
- (*c*) for the purposes of the *Criminal Records Act*, the finding of guilt in respect of the offence for which the record is kept is deemed to be a conviction.

Records of Offences that Result in a Prohibition Order
(10) Despite anything in this Act, when a young person is found guilty of an offence that results in a prohibition order being made, and the order is still in force at the end of the applicable period for which access to a record kept in respect of the order may be given under subsection (2):

- (*a*) the record kept by the Royal Canadian Mounted Police pursuant to subsection 115(3) may be disclosed only to establish the existence of the order for purposes of law enforcement; and
- (*b*) the record referred to in section 114 that is kept by the youth justice court may be disclosed only to establish the existence of the order in any offence involving a breach of the order.

- 2002, c. 1, s. 119;
- 2012, c. 1, ss. 157, 191(F).

Access to R.C.M.P. Records
120. (1) The following persons may, during the period set out in subsection (3), be given access to a record kept under subsection 115(3) in respect of an offence set out in the schedule:

- (*a*) the young person to whom the record relates;
- (*b*) the young person's counsel, or any representative of that counsel;
- (*c*) an employee or agent of the Government of Canada, for statistical purposes under the *Statistics Act*;
- (*d*) any person or member of a class of persons that a youth justice court judge considers has a valid interest in the record, to the extent directed by the judge, if the judge is satisfied that access is desirable in the public interest for research or statistical purposes;
- (*e*) the Attorney General or a peace officer, when the young person is or has been charged with another offence set out in the schedule or the same offence more than once, for the purpose of investigating any offence that the young person is suspected of having committed, or in respect of which the young person has been arrested or charged, whether as a young person or as an adult;
- (*f*) the Attorney General or a peace officer to establish the existence of an order in any offence involving a breach of the order; and
- (*g*) any person for the purposes of the *Firearms Act*.

Access for Identification Purposes
(2) During the period set out in subsection (3), access to the portion of a record kept under subsection 115(3) that contains the name, date of birth and last known address of the young person to whom the fingerprints belong, may be given to a person for identification purposes if a fingerprint identified as that of the young person is found during the investigation of an offence or during an attempt to identify a deceased person or a person suffering from amnesia.

Period of Access

(3) For the purposes of subsections (1) and (2), the period of access to a record kept under subsection 115(3) in respect of an offence is the following:

- (*a*) if the offence is an indictable offence, other than an offence referred to in paragraph (*b*), the period starting at the end of the applicable period set out in paragraphs 119(2)(*h*) to (*j*) and ending five years later; and
- (*b*) if the offence is a serious violent offence for which the Attorney General has given notice under subsection 64(2) (intention to seek adult sentence), the period starting at the end of the applicable period set out in paragraphs 119(2)(*h*) to (*j*) and continuing indefinitely.

Subsequent Offences as Young Person

(4) If a young person was found guilty of an offence set out in the schedule is, during the period of access to a record under subsection (3), found guilty of an additional offence set out in the schedule, committed when he or she was a young person, access to the record may be given to the following additional persons:

- (*a*) a parent of the young person or any adult assisting the young person under subsection 25(7);
- (*b*) a judge, court or review board, for a purpose relating to proceedings against the young person under this Act or any other Act of Parliament in respect of offences committed or alleged to have been committed by the young person, whether as a young person or as an adult; or
- (*c*) a member of a department or agency of a government in Canada, or of an organization that is an agent of, or is under contract with, the department or agency, who is:
  - (i) preparing a report in respect of the young person under this Act or for the purpose of assisting a court in sentencing the young person after the young person becomes an adult,
  - (ii) engaged in the supervision or care of the young person, whether as a young person or as an adult, or in the administration of a sentence in respect of the young person, whether as a young person or as an adult, or
  - (iii) considering an application for conditional release, or for a record suspension under the *Criminal Records Act*, made by the young person after the young person becomes an adult.

Disclosure for Research or Statistical Purposes

(5) A person who is given access to a record under paragraph (1)(*c*) or (*d*) may subsequently disclose information contained in the record, but shall not disclose the information in any form that would reasonably be expected to identify the young person to whom it relates.

Subsequent Offences as Adult

(6) If, during the period of access to a record under subsection (3), the young person is convicted of an additional offence set out in the schedule, committed when he or she was an adult:

- (*a*) this Part no longer applies to the record and the record shall be dealt with as a record of an adult and may be included on the automated criminal conviction records retrieval system maintained by the Royal Canadian Mounted Police; and
- (*b*) for the purposes of the *Criminal Records Act*, the finding of guilt in respect of the offence for which the record is kept is deemed to be a conviction.

Deemed Election
121. For the purposes of sections 119 and 120, if no election is made in respect of an offence that may be prosecuted by indictment or proceeded with by way of summary conviction, the Attorney General is deemed to have elected to proceed with the offence as an offence punishable on summary conviction.

Disclosure of Information and Copies of Record
122. A person who is required or authorized to be given access to a record under section 119, 120, 123 or 124 may be given any information contained in the record and may be given a copy of any part of the record.

Where Records May be Made Available
123. (1) A youth justice court judge may, on application by a person after the end of the applicable period set out in subsection 119(2), order that the person be given access to all or part of a record kept under sections 114 to 116 or that a copy of the record or part be given to that person,

- (*a*) if the youth justice court judge is satisfied that:
  - (i) the person has a valid and substantial interest in the record or part,
  - (ii) it is necessary for access to be given to the record or part in the interest of the proper administration of justice, and
  - (iii) disclosure of the record or part or the information in it is not prohibited under any other Act of Parliament or the legislature of a province; or
- (*b*) if the youth court judge is satisfied that access to the record or part is desirable in the public interest for research or statistical purposes.

Restriction for Paragraph (1)(*a*)
(2) Paragraph (1)(*a*) applies in respect of a record relating to a particular young person or to a record relating to a class of young persons only if the identity of young persons in the class at the time of the making of the application referred to in that paragraph cannot reasonably be ascertained and the disclosure of the record is necessary for the purpose of investigating any offence that a person is suspected on reasonable grounds of having committed against a young person while the young person is, or was, serving a sentence.

Notice
(3) Subject to subsection (4), an application for an order under paragraph (1)(*a*) in respect of a record shall not be heard unless the person who makes the application has given the young person to whom the record relates and the person or body that has possession of the record at least five days' notice in writing of the application, and the young person and the person or body that has possession have had a reasonable opportunity to be heard.

Where Notice Not Required
(4) A youth justice court judge may waive the requirement in subsection (3) to give notice to a young person when the judge is of the opinion that:

- (*a*) to insist on the giving of the notice would frustrate the application; or
- (*b*) reasonable efforts have not been successful in finding the young person.

Use of Record
(5) In any order under subsection (1), the youth justice court judge shall set out the purposes for which the record may be used.

Disclosure for Research or Statistical Purposes
(6) When access to a record is given to any person under paragraph (1)(*b*), that person may subsequently disclose information contained in the record, but shall not disclose the information in any form that would reasonably be expected to identify the young person to whom it relates.

Access to Record by Young Person
124. A young person to whom a record relates and his or her counsel may have access to the record at any time.

Disclosure of Information in a Record

Disclosure by Peace Officer During Investigation

- **125.** (1) A peace officer may disclose to any person any information in a record kept under section 114 (court records) or 115 (police records) that it is necessary to disclose in the conduct of the investigation of an offence.

Disclosure by Attorney General
(2) The Attorney General may, in the course of a proceeding under this Act or any other Act of Parliament, disclose the following information in a record kept under section 114 (court reports) or 115 (police records):

  - (*a*) to a person who is a co-accused with the young person in respect of the offence for which the record is kept, any information contained in the record; and
  - (*b*) to an accused in a proceeding, if the record is in respect of a witness in the proceeding, information that identifies the witness as a young person who has been dealt with under this Act.

Information that may be Disclosed to a Foreign State
(3) The Attorney General or a peace officer may disclose to the Minister of Justice of Canada information in a record that is kept under section 114 (court records) or 115 (police records) to the extent that it is necessary to deal with a request to or by a foreign state under the *Mutual Legal Assistance in Criminal Matters Act*, or for the purposes of any extradition matter under the *Extradition Act*. The Minister of Justice of Canada may disclose the information to the foreign state in respect of which the request was made, or to which the extradition matter relates, as the case may be.

Disclosure to Insurance Company
(4) A peace officer may disclose to an insurance company information in a record that is kept under section 114 (court records) or 115 (police records) for the purpose of investigating a claim arising out of an offence committed or alleged to have been committed by the young person to whom the record relates.

Preparation of Reports
(5) The provincial director or a youth worker may disclose information contained in a record if the disclosure is necessary for procuring information that relates to the preparation of a report required by this Act.

Schools and Others
(6) The provincial director, a youth worker, the Attorney General, a peace officer or any other person engaged in the provision of services to young persons may disclose to any professional or other person engaged in the supervision or care of a young person — including a representative of any school board or school or any other educational or training institution — any information contained in a record kept under sections 114 to 116 if the disclosure is necessary

- (*a*) to ensure compliance by the young person with an authorization under section 91 or an order of the youth justice court;
- (*b*) to ensure the safety of staff, students or other persons; or
- (*c*) to facilitate the rehabilitation of the young person.

Information to be Kept Separate
(7) A person to whom information is disclosed under subsection (6) shall

- (*a*) keep the information separate from any other record of the young person to whom the information relates;
- (*b*) ensure that no other person has access to the information except if authorized under this Act, or if necessary for the purposes of subsection (6); and
- (*c*) destroy their copy of the record when the information is no longer required for the purpose for which it was disclosed.

Time Limit
(8) No information may be disclosed under this section after the end of the applicable period set out in subsection 119(2) (period of access to records).

Records in the Custody, etc., of Archivists
126. When records originally kept under sections 114 to 116 are under the custody or control of the Librarian and Archivist of Canada or the archivist for any province, that person may disclose any information contained in the records to any other person if

- (*a*) a youth justice court judge is satisfied that the disclosure is desirable in the public interest for research or statistical purposes; and
- (*b*) the person to whom the information is disclosed undertakes not to disclose the information in any form that could reasonably be expected to identify the young person to whom it relates.

Disclosure with Court Order

- **127.** (1) The youth justice court may, on the application of the provincial director, the Attorney General or a peace officer, make an order permitting the applicant to disclose to the person or persons specified by the court any information about a young person that is specified, if the court is satisfied that the disclosure is necessary, having regard to the following circumstances:
  - (*a*) the young person has been found guilty of an offence involving serious personal injury;
  - (*b*) the young person poses a risk of serious harm to persons; and
  - (*c*) the disclosure of the information is relevant to the avoidance of that risk.

Opportunity to be Heard
(2) Subject to subsection (3), before making an order under subsection (1), the youth justice court shall give the young person, a parent of the young person and the Attorney General an opportunity to be heard.

***Ex parte* Application**
(3) An application under subsection (1) may be made *ex parte* by the Attorney General where the youth justice court is satisfied that reasonable efforts have been made to locate the young person and that those efforts have not been successful.

Time Limit
(4) No information may be disclosed under subsection (1) after the end of the applicable period set out in subsection 119(2) (period of access to records).

Disposition or Destruction of Records and Prohibition on Use and Disclosure

Effect of end of Access Periods
128. (1) Subject to sections 123, 124 and 126, after the end of the applicable period set out in section 119 or 120 no record kept under sections 114 to 116 may be used for any purpose that would identify the young person to whom the record relates as a young person dealt with under this Act or the *Young Offenders Act*, chapter Y-1 of the Revised Statutes of Canada, 1985.

Disposal of Records
(2) Subject to paragraph 125(7)(*c*), any record kept under sections 114 to 116, other than a record kept under subsection 115(3), may, in the discretion of the person or body keeping the record, be destroyed or transmitted to the Librarian and Archivist of Canada or the archivist for any province, at any time before or after the end of the applicable period set out in section 119.

Disposal of R.C.M.P. Records
(3) All records kept under subsection 115(3) shall be destroyed or, if the Librarian and Archivist of Canada requires it, transmitted to the Librarian and Archivist, at the end of the applicable period set out in section 119 or 120.

Purging CPIC
(4) The Commissioner of the Royal Canadian Mounted Police shall remove a record from the automated criminal conviction records retrieval system maintained by the Royal Canadian Mounted Police at the end of the applicable period referred to in section 119; however, information relating to a prohibition order made under an Act of Parliament or the legislature of a province shall be removed only at the end of the period for which the order is in force.

Exception
(5) Despite subsections (1), (2) and (4), an entry that is contained in a system maintained by the Royal Canadian Mounted Police to match crime scene information and that relates to an offence committed or alleged to have been committed by a young person shall be dealt with in the same manner as information that relates to an offence committed by an adult for which a record suspension ordered under the *Criminal Records Act* is in effect.

Authority to Inspect
(6) The Librarian and Archivist of Canada may, at any time, inspect records kept under sections 114 to 116 that are under the control of a government institution as defined in section 2 of the *Library and Archives of Canada Act*, and the archivist for a province may at any time inspect any records kept under those sections that the archivist is authorized to inspect under any Act of the legislature of the province.

- Definition of “destroy”

(7) For the purposes of subsections (2) and (3), “destroy”, in respect of a record, means:

  - (*a*) to shred, burn or otherwise physically destroy the record, in the case of a record other than a record in electronic form; and
  - (*b*) to delete, write over or otherwise render the record inaccessible, in the case of a record in electronic form.

No Subsequent Disclosure
129. No person who is given access to a record or to whom information is disclosed under this Act shall disclose that information to any other person unless the disclosure is authorized under this Act.

Evidence (Youth Statements)

General Law on Admissibility of Statements to Apply

- **146.** (1) Subject to this section, the law relating to the admissibility of statements made by persons accused of committing offences applies in respect of young persons.

When Statements are Admissible

(2) No oral or written statement made by a young person who is less than eighteen years old, to a peace officer or to any other person who is, in law, a person in authority, on the arrest or detention of the young person or in circumstances where the peace officer or other person has reasonable grounds for believing that the young person has committed an offence is admissible against the young person unless:

- (*a*) the statement was voluntary;
- (*b*) the person to whom the statement was made has, before the statement was made, clearly explained to the young person, in language appropriate to his or her age and understanding, that
  - (i) the young person is under no obligation to make a statement,
  - (ii) any statement made by the young person may be used as evidence in proceedings against him or her,
  - (iii) the young person has the right to consult counsel and a parent or other person in accordance with paragraph (*c*), and
  - (iv) any statement made by the young person is required to be made in the presence of counsel and any other person consulted in accordance with paragraph (*c*), if any, unless the young person desires otherwise;
- (*c*) the young person has, before the statement was made, been given a reasonable opportunity to consult:
  - (i) with counsel, and
  - (ii) with a parent or, in the absence of a parent, an adult relative or, in the absence of a parent and an adult relative, any other appropriate adult chosen by the young person, as long as that person is not a co-accused, or under investigation, in respect of the same offence; and
- (*d*) if the young person consults a person in accordance with paragraph (*c*), the young person has been given a reasonable opportunity to make the statement in the presence of that person.

Exception in Certain Cases for Oral Statements

(3) The requirements set out in paragraphs (2)(*b*) to (*d*) do not apply in respect of oral statements if they are made spontaneously by the young person to a peace officer or other person in authority before that person has had a reasonable opportunity to comply with those requirements.

Waiver of Right to Consult

(4) A young person may waive the rights under paragraph (2) (*c*) or (*d*) but any such waiver

- (*a*) must be recorded on video tape or audio tape; or
- (*b*) must be in writing and contain a statement signed by the young person that he or she has been informed of the right being waived.

Waiver of Right to Consult

(5) When a waiver of rights under paragraph (2)(*c*) or (*d*) is not made in accordance with subsection (4) owing to a technical irregularity, the youth justice court may determine that the waiver is valid if it is satisfied that the young person was informed of his or her rights, and voluntarily waived them.

Admissibility of Statements
(6) When there has been a technical irregularity in complying with paragraphs (2) (*b*) to (*d*), the youth justice court may admit into evidence a statement referred to in subsection (2), if satisfied that the admission of the statement would not bring into disrepute the principle that young persons are entitled to enhanced procedural protection to ensure that they are treated fairly and their rights are protected.

Statements Made Under Duress are Inadmissible
(7) A youth justice court judge may rule inadmissible in any proceedings under this Act a statement made by the young person in respect of whom the proceedings are taken if the young person satisfies the judge that the statement was made under duress imposed by any person who is not, in law, a person in authority.

Misrepresentation of Age
(8) A youth justice court judge may in any proceedings under this Act rule admissible any statement or waiver by a young person if, at the time of the making of the statement or waiver:

- (*a*) the young person held himself or herself to be eighteen years old or older;
- (*b*) the person to whom the statement or waiver was made conducted reasonable inquiries as to the age of the young person and had reasonable grounds for believing that the young person was eighteen years old or older; and
- (*c*) in all other circumstances the statement or waiver would otherwise be admissible.

Parent, etc., Not a Person in Authority
(9) For the purpose of this section, a person consulted under paragraph (2) (*c*) is, in the absence of evidence to the contrary, deemed not to be a person in authority.

Appendix B: Justice Department Canada on Bill C-13

Protecting Canadians from Online Crime Act
Since the introduction of Bill C-13, the *Protecting Canadians from Online Crime Act*, a number of misconceptions have developed around the intent and scope of this bill. I would like to clarify why this bill is necessary and why it is imperative that the bill address not only serious acts of cyberbullying but also the tools law enforcement officers need to investigate this and other online crime.

Why this Bill is necessary
Bill C-13 addresses a gap in the Criminal Code by making it illegal to distribute an intimate image of a person without their consent. But it is not enough to make this act a crime if we do not also update our current laws so that law enforcement authorities can, in fact, be allowed to conduct an appropriate and lawful investigation. In fact, a report prepared by a working group of Federal-Provincial-Territorial officials, released this past July, recommended both the creation of the new offence and modernizing the Criminal Code to provide police and prosecutors with judicially-authorized tools to investigate offences that are committed via the Internet or that involve electronic evidence. After all, there is no point in creating a law without giving law enforcement access to the very tools they need to investigate the offence.

In her November 28, 2013 statement on Bill C-13, the outgoing federal Privacy Commissioner Jennifer Stoddart commended the government "for recognizing the gravity of privacy intrusions online, and for proposing action to address the issue of cyberbullying." She also recognized that "law enforcement authorities need up-to-date tools to fight online crime at a time of when technologies are changing rapidly" and that this must be done in a way that respects Canadians' fundamental right to privacy.

This legislation respects privacy
It has been suggested that Bill C-13 is simply a new version of the old Bill C-30. To be clear, the new legislation does not include former Bill C-30's controversial amendments that would have allowed access to subscriber information without a warrant and would have called for telecommunication infrastructure modification to implement and maintain a technical capability to enable lawfully authorized interceptions. Bill C-13 simply aims to provide police with the necessary means to fight crime in today's high-tech environment while maintaining the judicial checks and balances needed to protect Canadians' privacy. There would still be a requirement for appropriate judicial oversight. Police could not access the different types of data included in the legislation without a judicial authorization.

The different parts of this legislation logically go together
There is a misconception that Bill C-13 is an omnibus crime bill. This is simply not accurate. Bill C-13 combines a proposed new offence of non-consensual distribution of intimate images to address cyberbullying with judicially-authorized tools to help police and prosecutors investigate the proposed new offence and other existing offences that are committed via the Internet or that involve electronic evidence. Both of these elements were recommended in the July 2013 Federal-Provincial-Territorial report on cyberbullying and the non-consensual distribution of intimate images.

It is already legal to provide information to the police
Some people mistakenly believe that the new legislation would allow the police to sidestep court authorization requirements by requesting voluntary disclosure or voluntary preservation of documents or data from organizations such as telecommunications service providers and banks. In this regard, the proposed legislation would not provide the police with any new powers. The Bill proposes small

revisions to the current law, to make it clearer in what circumstances the police do not require production orders if a third party voluntarily assists in a police investigation by providing information. As part of their general policing duties, police may already obtain information from a third party voluntarily without a court order. There is no need for the police to obtain production orders when persons were providing their assistance on a voluntary basis, as long as there was no prohibition against doing so, such as a duty to safeguard personal information under the *Personal Information Protection and Electronic Documents Act.*

Bill C-13 now explicitly refers to the protections from civil and criminal liability when a person chooses to provide voluntary assistance to the police—that is to say that a person who discloses information could not be sued or prosecuted for voluntarily providing information that they are not prohibited from disclosing. This protection already exists under the Criminal Code. This is not a substantive change, but was done to make the provision more transparent and understandable on its face.

This provision will also be amended to refer to the new proposed preservation demands and preservation orders into the Criminal Code, so as to clarify that a person may also voluntarily preserve data, so long as doing so is not otherwise prohibited.

Bill C-13 also proposes to clarify that voluntary cooperation with police is not restricted to when they are enforcing a federal law but that it also applies to police activities that do not directly relate to enforcing a federal law, such as contacting the next-of-kin of an accident victim, returning stolen property to its owner or contacting the home owner, in the case of a break-in.

Police are better able to keep Canadians safe and to investigate criminal activity when persons, groups and organizations are willing to assist them. The purpose of the current law and these updates relating to voluntary disclosure is to ensure that police and the public can continue to work cooperatively.

Tracking Devices

With respect to concerns that have been **raised** about tracking devices, it is important to note that the Bill retains judicial oversight for these devices. Police use a tracking device to track persons or things if the court has agreed to this activity and granted the necessary authority. Historical tracking data, which might show where a suspect has been in the past, would only be available to police subject to a valid judicial production order if there was reason to suspect that a criminal offence had been or will be committed. For real-time tracking of a person, Bill C-13 proposes to raise the level of judicial scrutiny from reasonable suspicion to reasonable belief. This is to reflect advances in technology which have increased the precision of tracking devices. I believe this represents a significant privacy safeguard for the use of this power.

It is Already Illegal to Steal Cable

Some reports have suggested that the new legislation would make it illegal to steal cable signals. In fact, the theft of telecommunications, including cable, and the possession of a device to obtain a telecommunication service without payment have long been offences under the criminal law.

The amendments proposed in Bill C-13 to these long-standing offences are amendments consistent with our efforts to modernize the Criminal Code and to make related provisions consistent with each other. This is not a substantive change.

It is important to note that the Bill would also make the offence of possession of software or other device to obtain a telecommunication service without payment a hybrid/dual procedure offence—this means that it would give prosecutors **more** discretion in their charging practices depending on the seriousness of the offence.

Hate Crimes

There have also been some concerns raised about the amendment to the definition of "identifiable group." The Bill proposes to amend the definition of "identifiable group" in the Criminal Code by including national origin, age, sex, and mental or physical disability in addition to the characteristics already provided by the Criminal Code, namely colour, race, religion, ethnic origin and sexual orientation. This would provide broader protection under the three Criminal Code offences relating to hate propaganda (i.e., genocide, public incitement of hatred, and willful promotion of hatred). The modification to add age, sex and mental or physical disability aims to address what could be seen as a gap resulting from changes to the *Canadian Human Rights Act* to delete section 13 of that *Act*.

Cyberbullying goes far beyond schoolyard bullying and, as our Prime Minister stated, can amount to a criminal activity. With the click of a button, a person can be victimized before the entire world. As we have seen far too often, such conduct can destroy lives. The resulting harm of online bullying is even believed to be a factor in the tragic suicides of several Canadian teenagers. It clearly demands a stronger criminal justice response and Bill C-13 proposes what is needed to address this behaviour, no more, no less.

Our Government believes in standing up for Canadians—because it is a basic right for children to feel protected—be it riding a bike in the neighbourhood or surfing the net. Bullying and cyberbullying are complex social problems that require action on a number of levels, from addressing gaps in the Criminal Code to prevention and education programs.

It is my firm belief that we can do more, which is what the *Protecting Canadians from Online Crime Act* is all about. I urge Parliamentarians and all Canadians to support this important step in protecting our children and youth online.

The Honourable Peter MacKay
Minister of Justice and Attorney General of Canada
Date Modified:
2013-12-12
Government of Canada Department of Justice News Release
http://www.justice.gc.ca/eng/news-nouv/nr-cp/2013/doc_33010.html

Appendix C: Resource Information and Areas for Exploration:

British Columbia

- https://reportbullyingbc.edudata.ca/apps/bullying/ **Erase Reporting Tool** - **every child deserves an education free from discrimination, bullying, harassment, intimidation and violence.** The ERASE (Expect Respect and A Safe Education) Bullying strategy is part of the Province of British Columbia's efforts to personalize learning and supports for all students.
- http://bc.rcmp-grc.gc.ca - RCMP resource - **iSMART** (Internet + Social Media Awareness Resource Toolkit) contains the information police officers need to understand and present on Internet and social media safety. For additional information, please contact "E" Division Crime Prevention Services. Phone: 778-290-4005.

Canadian

- www.mediasmarts.ca **MediaSmarts** has been developing digital and media literacy programs and resources for Canadian homes, schools and communities since 1996. Through their work they support adults with information and tools so they can help children and teens develop the critical thinking skills they need for interacting with the media they love.

- http://www.ycja.ca/police Police and Professionals can receive a certificate of completion from the Justice Education Society for achieving a passing score **of 80%** on the final exam. To register for this certificate, create an account. Already have an account? Log in.

Canadian Centre for Child Protection:

- www.Cybertip.ca **–Cybertip.ca's** mandate is to protect children from online sexual exploitation by receiving and processing tips from the public about potentially illegal material, as well as activities regarding the online sexual exploitation of children, and referring any relevant leads to the appropriate law enforcement agency and/or child welfare agency; and providing the public with information and other resources, as well as support and referral services, to help Canadians keep themselves and their families safe while using the Internet.

- www.thedoorthatsnotlocked.ca/app Committed to helping parents, teachers, and anyone else who would like to better understand the good, the bad, and the ugly about the web. **The Door that's not Locked** website has been created to provide a one-stop-shop on all things related to Internet safety including a variety of resources and tools that will help you keep your child safer while they're exploring and enjoying the online world.

- www.kidsintheknow.ca **Kids in the Know** is an interactive safety education program for increasing the personal safety of children and reducing their risk of sexual exploitation. Child sexual abuse is a

serious problem within our society and occurs more frequently than people realize. It is important to understand what child sexual abuse is and how to recognize behaviours that may signal a child in distress. Adults have an obligation to protect children from sexual abuse.

- www.Needhelpnow.ca Provides help for individuals (and their friends, peers or siblings) who have been involved in a self/peer exploitation incident (otherwise known as "sexting"). This site provides guidance on steps you can take to get through this.

Other Important Resources

- www.catsmi.ca **Canadian Access to Social Media Information Project**: funded by Office of the Privacy Commissioner of Canada. Provides specific information relevant to Canadian Jurisdiction and Legal Strategies (e.g. production orders, preservation orders, MLATS, etc.)

- https://wisefootprint.telus.com A fun way for Canadian tweens and teens to explore how to keep their digital footprint clean.

- http://www.rcmp-grc.gc.ca/cycp-cpcj RCMP Centre for youth crime prevention page providing Canadians with evidence-informed and age appropriate crime prevention messages, information, tools, and programs to prevent youth crime and victimization and motivate youth to think critically, build positive decision making skills and make changes in their lives and communities.

- www.redcross.ca/what-we-do Provides violence, bullying and abuse prevention programs including Beyond the Hurt, a dynamic online educational program designed to help create and maintain positive, inclusive environments

- www.getcybersafe.gc.ca Government of Canada website for Parents and Teens providing information on a range of online topics including cyber bullying, online identity and current scams, frauds, and online threats.

- www.missingkids.ca Offering families support in finding their missing child and provide educational materials to help prevent children from going missing.

International

- www.netsmartz.org **NetSmartz Workshop** is an interactive, educational program of the National Center for Missing & Exploited Children® (NCMEC) that provides age-appropriate resources to help teach children how to be safer on, and offline. The program is designed for children ages 5-17, parents and guardians, educators, and law enforcement. With resources such as videos, games, activity cards, and presentations, NetSmartz entertains while it educates.

- www.wordswound.org - Cyberbullying specific prevention for youth. 'The Street Team' is a free online space for supporters who want to spread the message by doing their part. It's a practical, effective way for supporters to make a difference every day, in whatever way they can. It doesn't matter where they are, street team members can help out in their schools, neighborhoods, local venues, even from behind your tablet or phone.

- www.safesurf.com **SafeSurf** is an internet voluntary rating standard devoted to building a safe Internet. It provides a wide variety of products, services and information and an opportunity to get your own website content rated for free.

- www.commonsensemedia.org **Common Sense Media** is an independent advocate for improving the media landscape for kids and families. They work with lawmakers and other policymakers nationwide in support of policies that empower parents, teachers, and young people to harness the power of technology safely and responsibly, while keeping personal information private and protected.

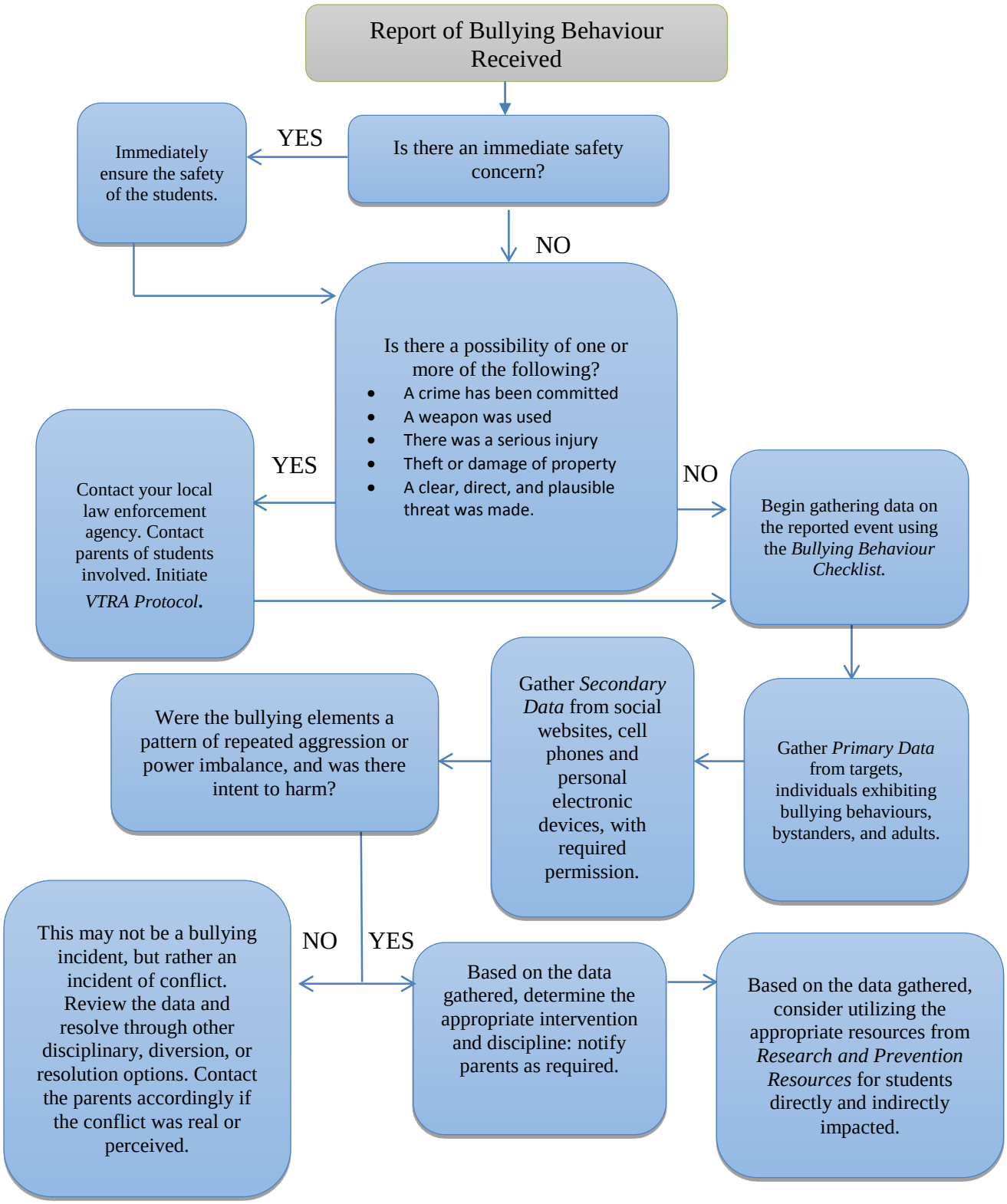
Resources for Victims of Cyberbullying:

Removal of posts/images: www.needhelpnow.ca

Support for Victims: http://needhelpnow.ca/app/en/coping
http://www.victimlinkbc.ca

Education to prevent further victimization:
http://mediasmarts.ca/sites/default/files/pdfs/tipsheet/TipSheet_Think_Before_You_Share.pdf

Appendix D: Bullying Flowchart (Safer Schools Together, SST)



Appendix E: Cyberbullying Checklist

School-Based Bullying Incident Checklist

Checklist Completed By:

Name: **Date:**

Students Involved:

Victim(s)	Bully(ies)	Helpful Bystander(s)	Hurtful Bystander(s)

Indicate the section of School District policy that has been breached:

School Act - Preamble, Sections 2, 6(1), 75(1), 76(2)(3), 85(1)(1.1)(2), 169(3), and 177.

Incident Synopsis

Physical Bullying	Verbal Bullying	Social-Diversity-Relational Bullying	Cyber Bullying
☐	☐	☐	☐
Refer to Resource App One	Refer to Resource App One	Refer to Resource App Two	Refer to Resource App Three

Narrative

Incident Management

	Yes	No
Do parents need to been notified?	☐	☐
Do Superintendents need to be notified?	☐	☐
Do police need to be notified?	☐	☐
Have cell phones been checked for pictures, videos and text?	☐	☐
Have social media sites been checked for pictures, video, and text?	☐	☐

Incident Intervention

	Yes	No
Will student discipline be required?	☐	☐
Are alternatives to discipline appropriate?	☐	☐
Have school based resources been accessed?	☐	☐
Have district resources been accessed?	☐	☐
Have community resources been accessed?	☐	☐
Is school or classroom education required?	☐	☐

Check in #1	☐	**2 Days after reported incident**
Check in #2	☐	**7 Days after reported incident**
Check in #3	☐	**14 Days after reported incident**
Check in #4	☐	**1 Month after reported incident**
Check in #5	☐	**As required**
Check in #6	☐	**As required**

Appendix F: OPC Complaint Form

***Personal Information Protection and Electronic Documents Act* (PIPEDA)**
Complaint Form

SECTION 1: Complainant / Representative Information

If you are the complainant, you should complete the section "Complainant Information."

If you represent the complainant, you should complete the sections "Complainant Information" and "Representative Information," as well as the authorization form available on our website.

1. Are you making this complaint on your own behalf? * ☐ Yes ☐ No

If 'No', please make sure that you send us a written authorization from the person you are representing.

Complainant Information

First name *	Last name *	Email address
Mailing address *		City *
Province *	Postal code *	Country (if outside Canada)
Daytime Telephone number *	Alternative Telephone number	
Please enter the Daytime Telephone Number as the best number to contact you from Monday to Friday, 8:30am to 4:30pm ET.		

Representative Information *(if applicable)*

First name *	Last name *	Email address
Mailing address *		City *
Province *	Postal code *	Country (if outside Canada)
Daytime Telephone number *	Alternative Telephone number	
Please enter the Daytime Telephone Number as the best number to contact you from Monday to Friday, 8:30am to 4:30pm ET.		

* Required fields

SECTION 2: Details of Complaint
Please provide information about your complaint below.
You should also describe any efforts you made to resolve the issue with the organization concerned.

2. Which organization is your complaint against? * *(Please identify by specific name and location. Provide legal name of organization, if known.)*

3. Are you submitting the complaint as a customer or as an employee of the organization? *
☐ Customer ☐ Employee

4. Summarize your complaint. * *(Please describe the events or circumstances that led to your complaint. Include details such as the names or positions of people involved in the incident, the locations where the incident occurred, and any other factors you consider relevant. If the organization gave you a reference number in relation to this issue, please include it as well.*)

5. Have you attempted to resolve the matter with the organization?
☐ Yes ☐ No

If 'Yes', please outline your efforts and describe the result, if any. If 'No', please specify the reason why not.

6. Have you complained about this incident to another body or organization?
☐ Yes ☐ No

If 'Yes', please provide details. *(Indicate the name of the body, and include relevant details such as dates and a reference number.)*

7. How can the Office of the Privacy Commissioner of Canada help address your concerns? *
(*Please describe any steps or remedies that would resolve your issue.*)

* Required fields

SECTION 3: Documentation
If you have documents relating to your complaint, please attach them to your complaint:
Any correspondence between you and the organization on this matter.
Any documentation that indicates that you are authorized to act for another person (authorization form).
Other relevant documentation.

☐ Documents will be sent under separate cover to the address or fax number below
☐ Documents attached

Please list the file names of the attached documents.

SECTION 4: Certification
By signing this form, you certify that the information you provided on this form, to the best of your knowledge, is true and complete.

_____
First and last names (print)

_____ _____
Signature Date (dd/mm/yyyy)

Send Complaint Form to:

Office of the Privacy Commissioner of Canada
30 Victoria Street
Gatineau, Quebec
K1A 1H3

Inquiries:
Toll-free: 1-800-282-1376
Phone: (819) 994-5444
TTY: (819) 994-6591

The personal information you provide on this form is protected under the provisions of the *Access to Information Act* and the *Privacy Act*. Please note that your name and the details of your complaint will be shared with the organization that is the subject of the complaint.

Appendix G: Law Enforcement Guide for Facebook

Accessed 21/07/2015 from https://www.facebook.com/safety/groups/law/guidelines/

These operational guidelines are for law enforcement officials seeking records from Facebook. For private party requests, including requests from civil litigants and criminal defendants, visit: facebook.com/help/?page=1057. Users seeking information on their own accounts can access Facebook's "Download Your Information" feature from their account settings. See facebook.com/help/?page=18830. This information may change at any time.

US Legal Process Requirements

We disclose account records solely in accordance with our terms of service and applicable law, including the federal Stored Communications Act ("SCA"), 18 U.S.C. Sections 2701-2712. Under US law:

- A valid subpoena issued in connection with an official criminal investigation is required to compel the disclosure of basic subscriber records (defined in 18 U.S.C. Section 2703(c)(2)), which may include: name, length of service, credit card information, email address(es), and a recent login/logout IP address(es), if available.
- A court order issued under 18 U.S.C. Section 2703(d) is required to compel the disclosure of certain records or other information pertaining to the account, not including contents of communications, which may include message headers and IP addresses, in addition to the basic subscriber records identified above.
- A search warrant issued under the procedures described in the Federal Rules of Criminal Procedure or equivalent state warrant procedures upon a showing of probable cause is required to compel the disclosure of the stored contents of any account, which may include messages, photos, videos, wall posts, and location information.
- We interpret the national security letter provision as applied to Facebook to require the production of only 2 categories of information: name and length of service.

International Legal Process Requirements

We disclose account records solely in accordance with our terms of service and applicable law. A Mutual Legal Assistance Treaty request or letter rogatory may be required to compel the disclosure of the contents of an account. Further information can be found here:facebook.com/about/privacy/other.

Account Preservation

We will take steps to preserve account records in connection with official criminal investigations for 90 days pending our receipt of formal legal process. You may expeditiously submit formal preservation requests through the Law Enforcement Online Request System at facebook.com/records, or by email, or mail as indicated below.

Emergency Requests
In responding to a matter involving imminent harm to a child or risk of death or serious physical injury to any person and requiring disclosure of information without delay, a law enforcement official may submit a request through the Law Enforcement Online Request System at facebook.com/records. Important note: We will not review or respond to messages sent to this email address by non-law enforcement officials. Users aware of an emergency situation should immediately and directly contact local law enforcement officials.

Child Safety Matters
We report all apparent instances of child exploitation appearing on our site from anywhere in the world to the National Center for Missing and Exploited Children (NCMEC), including content drawn to our attention by government requests. NCMEC coordinates with the International Center for Missing and Exploited Children and law enforcement authorities from around the world. If a request relates to a child exploitation or safety matter, please specify those circumstances (and include relevant NCMEC report identifiers) in the request to ensure that we are able to address these matters expeditiously and effectively.

Data Retention and Availability
We will search for and disclose data that is specified with particularity in an appropriate form of legal process and which we are reasonably able to locate and retrieve. We do not retain data for law enforcement purposes unless we receive a valid preservation request before a user has deleted that content from our service.

Details about data and account deletion can be found in our Data Use Policy(facebook.com/policy.php), Statement of Rights and Responsibilities(facebook.com/terms.php), and Help Center (facebook.com/help/?faq=224562897555674).

Form of Requests

We will be unable to process overly broad or vague requests. All requests must identify requested records with particularity and include the following:

- The name of the issuing authority, badge/ID number of responsible agent, email address from a law-enforcement domain, and direct contact phone number.
- The email address, user ID number (http://www.facebook.com/profile.php?id=1000000XXXXXXXX) or username (http://www.facebook.com/username) of the Facebook profile.

User Consent
If a law enforcement official is seeking information about a Facebook user who has provided consent for the official to access or obtain the user's account information, the user should be directed to obtain that information on their own from their account. For account content, such as messages, photos, videos and wall posts, users can access Facebook's

“Download Your Information” feature from their account settings.
See facebook.com/help/?page=18830. Users can also view recent IP addresses in their Account Settings under Security Settings/Active Sessions. Users do not have access to historical IP information without legal process.

Notification
Our policy is to notify people who use our service of requests for their information prior to disclosure unless we are prohibited by law from doing so or in exceptional circumstances, such as child exploitation cases, emergencies or when notice would be counterproductive. We will provide delayed notice upon expiration of a specific non-disclosure period in a court order and where we have a good faith belief that exceptional circumstances no longer exist and we are not otherwise prohibited by law from doing so. Law enforcement officials who believe that notification would jeopardize an investigation should obtain an appropriate court order or other appropriate process establishing that notice is prohibited. If your data request draws attention to an ongoing violation of our terms of use, we will take action to prevent further abuse, including actions that may notify the user that we are aware of their misconduct.

Testimony
Facebook does not provide expert testimony support. In addition, Facebook records are self-authenticating pursuant to law and should not require the testimony of a records custodian. If a special form of certification is required, please attach it to your records request.

Cost Reimbursement
We may seek reimbursement for costs in responding to requests for information as provided by law. These fees apply on a per account basis. We may also charge additional fees for costs incurred in responding to unusual or burdensome requests.

We may waive these fees in matters investigating potential harm to children, Facebook and our users, and emergency requests.

Submission of Requests
Online
Law enforcement officials may use the Law Enforcement Online Request System atfacebook.com/records for the submission, tracking and processing of requests.

Please note that a government-issued email address is required to access the Law Enforcement Online Request System. You may also submit requests by email as indicated below.

Mail
United States Mailing Address: 1601 Willow Road, Menlo Park CA 94025
Ireland Mailing Address: Facebook Ireland Ltd | 4 Grand Canal Square | Dublin 2

Attention: Facebook Security, Law Enforcement Response Team

Law enforcement officials who do not submit requests through the Law Enforcement Online Request System at facebook.com/records should expect longer response times.

Notes

- Acceptance of legal process by any of these means is for convenience and does not waive any objections, including lack of jurisdiction or proper service.
- We will not respond to correspondence sent by non-law enforcement officials to the addresses above.

Appendix H: Law Enforcement Guide for Instagram

Accessed 21/07/2015 from https://help.instagram.com/494561080557017/

These operational guidelines are for law enforcement officials seeking records from Instagram LLC, a wholly owned subsidiary of Facebook, Inc. This information may change at any time.

Requests for User Information

We disclose account records solely in accordance with our terms of service and applicable law, including the federal Stored Communications Act ("SCA"), 18 U.S.C. Sections 2701-2712. Under the SCA:

- a valid subpoena issued in connection with an official criminal investigation is required to compel the disclosure of basic subscriber records (defined in 18 U.S.C. Section 2703(c)(2)), which may include: subscriber name, account creation date, email address, and a signup IP address, if available.
- a court order issued under 18 U.S.C. Section 2703(d) is required to compel the disclosure of certain records or other information pertaining to the account, not including contents of communications, which may include photographs, photo captions, and other electronic communication information in addition to the basic subscriber records identified above.
- a search warrant issued under the procedures described in the Federal Rules of Criminal Procedure or equivalent State warrant procedures upon a showing of probable cause is required to compel the disclosure of the stored contents of any account, which may include messages, photos, comments, and location information.

It is important to note that some information we store is collected automatically, while other information is provided by the user. We do not require email or phone verification, and we do not require people to use real names or identities on Instagram.

For additional information about Instagram, please read our Privacy Policy and Terms of Use.

Data Retention and Availability

We retain different types of information for different time periods. Given the volume of real-time content on Instagram, some information may only be stored for a short period of time. We do not retain data for law enforcement purposes unless we receive a valid preservation request.

Information to Include

All requests must identify the following:

1. The name of the issuing authority, badge/ID number of responsible agent, email address from a law enforcement domain, and a direct contact phone number.
2. The username of the Instagram account in question on the date you viewed the account and details regarding specific information requested and its relationship to your investigation. Usernames are not static and we are unable to process

requests that do not include the date viewed combined with the username. If you have access to an image's short URL, you can go to the link and find the username at the top right next to the image. If you have access to the Instagram app, you can locate the username at the top of the account's profile.

Emergency Requests

In responding to a matter involving imminent harm to a child or risk of death or serious physical injury to any person and requiring disclosure of information without delay, a law enforcement official may submit a request through the Law Enforcement Online Request System at facebook.com/records.

Important note: We will not review or respond to messages sent to this email address by non-law enforcement officials. Users aware of an emergency situation should immediately and directly contact local law enforcement officials.

International Legal Process Requirements

We disclose account records solely in accordance with applicable terms of service and applicable law. A Mutual Legal Assistance Treaty request or letter rogatory may be required to compel the disclosure of the contents of an account. Further information can be found here: help.instagram.com/155833707900388/.

Account Preservation

We will take steps to preserve account records in connection with official criminal investigations for 90 days pending our receipt of formal legal process. You may expeditiously submit formal preservation requests through the Law Enforcement Online Request System at facebook.com/records, or by email, or mail as indicated below.

User Consent

If law enforcement seeks information about a an Instagram user who has provided consent for the official to access or obtain the user's account information, the user should be directed to obtain that information on their own from their account.

Notification

Our policy is to notify people who use our service of requests for their information prior to disclosure unless we are prohibited by law from doing so or in exceptional circumstances, such as child exploitation cases, emergencies or when notice would be counterproductive. We will provide delayed notice upon expiration of a specific non-disclosure period in a court order and where we have a good faith belief that exceptional circumstances no longer exist and we are not otherwise prohibited by law from doing so. Law enforcement officials who believe that notification would jeopardize an investigation should obtain an appropriate court order or other appropriate process establishing that notice is prohibited. If your data request draws attention to an ongoing violation of our terms of use, we will take action to prevent further abuse, including actions that may notify the user that we are aware of their misconduct.

Testimony

We are unable to provide expert testimony. Any records produced are self-authenticating and do not require the testimony of records custodians. If a special form of certification is required, please attach it to your records request.

Cost Reimbursement

We may seek reimbursement for costs in responding to requests for information as provided by law. Unusual or burdensome requests may result in added costs that we may recover. We may waive fees in matters pertaining to potential harm to children, us or our users, and emergency requests.

Submission of Requests

Online:

Law enforcement officials are encouraged to use the Law Enforcement Online Request System at facebook.com/records for the submission, tracking and processing of requests. Please note that a government-issued email address is required to access the Law Enforcement Online Request System.

Mail:

Attn: Law Enforcement Response Team
1601 Willow Road
Menlo Park, CA 94025

Email:

lawenforcement@instagram.com

Law enforcement officials who do not submit requests through the Law Enforcement Online Request System at facebook.com/records should expect longer response times.

Notes

- Acceptance of legal process by any of these means is for convenience and does not waive any objections, including lack of jurisdiction or improper service.
- We will not review or respond to correspondence sent by non-law enforcement officials to the addresses above.

Appendix I: Law Enforcement Guide for Twitter

Accessed 21/07/2015 from https://support.twitter.com/articles/41949-guidelines-for-law-enforcement

What is Twitter?

Twitter is a real-time global information network that lets users create and share ideas and information instantly. People and organizations send 140-character messages through our website and mobile site, client applications (e.g., Twitter for Android; Twitter for iOS), SMS, or any variety of third-party applications.

For more information, please visit: https://about.twitter.com. For the latest on Twitter's features and functionality please visit our Help Center.

Twitter is provided to people who live in the United States by Twitter, Inc., a company based in San Francisco, California. Twitter is provided to people who live outside the United States by Twitter International Company, a company based in Dublin, Ireland.

What Account Information Does Twitter Have?

Most Twitter account information is public, so anyone can see it. A Twitter account profile contains a profile photo, header photo, background image, and status updates, called Tweets. In addition, the account holder has the option to fill out a location (e.g., San Francisco), a URL (e.g., twitter.com), and a short "bio" section about the account for display on their public profile. Please see our Privacy Policy for more information on the data we collect from and about users.

Does Twitter Have Access to User-Generated Photos or Videos?

Twitter provides photo hosting for some image uploads (i.e., pic.twitter.com images) as well as Twitter account profile photos, header photos, and account background images. However, Twitter is not the sole photo provider for images that may appear on the Twitter platform. More information about posting photos on Twitter can be found here.

Twitter provides video hosting for some videos uploaded to Twitter (i.e., pic.twitter.com videos) as well as those posted to Periscope and Vine.

What is Periscope?

Periscope is a standalone mobile service that lets users create and share real-time video broadcasts. Please see the Periscope Privacy Statement for more information on the data we collect from and about Periscope users.

What is Vine?

Vine is a standalone mobile service that lets users create and share short looping videos. Please see the Vine Privacy Policy for more information on the data we collect from and about Vine users.

Data Retention Information

Twitter retains different types of information for different time periods, and in accordance with our Terms of Service and Privacy Policy. Given Twitter's real-time nature, some information (e.g., IP logs) may only be stored for a very brief period of time.

Some information we store is automatically collected, while other information is provided at the user's discretion. Though we do store this information, we cannot guarantee its accuracy. For example, the user may have created a fake or anonymous profile. Twitter doesn't require real name use, email verification, or identity authentication. More information on Twitter's retention policies can be found in our Privacy Policy.

NOTE: Once an account has been deactivated, there is a very brief period in which we may be able to access account information, including Tweets. More information about deactivated accounts is available here. Content deleted by account holders (e.g., Tweets) is generally not available.

Preservation Requests

We accept requests from law enforcement to preserve records, which constitute potentially relevant evidence in legal proceedings. We will preserve, but not disclose, a temporary snapshot of the relevant account records for 90 days pending service of valid legal process.

Preservation requests, in accordance with applicable law, should be signed by the requesting official, include the @username and URL of the subject Twitter profile (e.g., @safety and https://twitter.com/safety), have a valid return official email address, and be sent on law enforcement letterhead. Requests may be sent via the methods described below.

Requests for Twitter Account Information

Requests for user account information from law enforcement should be directed to Twitter, Inc. in San Francisco, California or Twitter International Company in Dublin, Ireland. Twitter responds to valid legal process issued in compliance with applicable law.

Private Information Requires a Subpoena or Court Order

Non-public information about Twitter users will not be released to law enforcement except in response to appropriate legal process such as a subpoena, court order, or other valid legal process – or in response to a valid emergency request, as described below.

Contents of Communications Requires a Search Warrant

Requests for the contents of communications (e.g., Tweets, Direct Messages, photos) require a valid search warrant or equivalent from an agency with proper jurisdiction over Twitter.

Will Twitter Notify Users of Requests for Account Information?

Yes. Twitter's policy is to notify users of requests for their account information, which includes a copy of the request, prior to disclosure unless we are prohibited from doing so (e.g., an order under 18 U.S.C. § 2705(b)). Exceptions to prior notice may include exigent or counterproductive circumstances (e.g., emergencies; account compromises). We may also provide post-notice to affected users when prior notice is prohibited.

What Details Must Be Included in Account Information Requests?

When requesting user account information, please include:

- The @username and URL of the subject Twitter account in question (e.g., @safety and https://twitter.com/safety);
- Details about what specific information is requested (e.g., basic subscriber information) and its relationship to your investigation;
    - **NOTE**: Please ensure that the information you seek is not available from our public API. We are unable to process overly broad or vague requests.
- A **valid official email address** (e.g., name@agency.gov) so we may get back in touch with you upon receipt of your legal process.

Requests may be submitted by fax or mail; our contact information is available at the bottom of these Guidelines. Requests must be made on law enforcement letterhead.

NOTE: We do **not** accept legal process via email at this time; our support system does not allow attachments for security reasons.

Production of Records

Unless otherwise agreed upon, we currently provide responsive records in electronic format (i.e., text files that can be opened with any word processing software such as Word or TextEdit).

Records Authentication

The records that we produce are self-authenticating. Additionally, the records are electronically signed to ensure their integrity at the time of production. If you require a declaration, please explicitly note that in your request.

Cost Reimbursement

Twitter may seek reimbursement for costs associated with information produced pursuant to legal process and as permitted by law (e.g., under 18 U.S.C. §2706

Emergency Disclosure Requests

In line with our Privacy Policy, we may disclose account information to law enforcement in response to a valid emergency disclosure request.

Twitter evaluates emergency disclosure requests on a case-by-case basis in compliance with relevant law (e.g., 18 U.S.C. § 2702(b)(8) and Section 8 Irish Data Protection 1988 and 2003). If we receive information that provides us with a good faith belief that there is an exigent emergency involving the danger of death or serious physical injury to a person, we may provide information necessary to prevent that harm, if we have it.

How To Make an Emergency Disclosure Request

If there is an exigent emergency that involves the danger of death or serious physical injury to a person that Twitter may have information necessary to prevent, **law enforcement officers can submit an emergency disclosure request through our web form** (the quickest and most efficient method).

Alternatively, you may fax emergency requests to 1-415-222-9958 (NOTE: faxed requests may result in a delayed response); please include all of the following information:

- Indication on your cover sheet, which must be on law enforcement letterhead, that you're submitting an Emergency Disclosure Request;
- Identity of the person who is in danger of death or serious physical injury;

- The nature of the emergency (e.g., report of suicide, bomb threat);
- Twitter @username and URL (e.g., @safety and https://twitter.com/safety) of the subject account(s) whose information is necessary to prevent the emergency;
- Any specific Tweets you would like us to review;
- The specific information requested and why that information is necessary to prevent the emergency;
- The signature of the submitting law enforcement officer; and
- All other available details or context regarding the particular circumstances.

Mutual Legal Assistance Treaties

Twitter's policy is to promptly respond to requests that are properly issued via mutual legal assistance treaty ("MLAT") or letters rogatory, upon proper service of process.

Assisting a Twitter User

Registered Twitter users can obtain a download of Tweets posted to his or her Twitter account. Directions on how a user can request that information is available in our Help Center.

Twitter does not currently offer users a self-serve method to obtain other, non-public information (e.g., IP logs) about their Twitter accounts. If a Twitter user requires his or her non-public account information, please direct the user to send a request to Twitter via our privacy form. We will respond with further instructions.

Other Issues

Most issues can be resolved by having Twitter account holders submit inquires directly to us through our Help Center. More information on how to report violations is available here.

General Inquiries

Other general inquiries from law enforcement or government officials can be submitted through our web form.

Contact Information

Our address and fax details are:

Twitter, Inc.
c/o Trust & Safety - Legal Policy
1355 Market Street, Suite 900
San Francisco, CA 94103
Fax: 1-415-222-9958 (attn: Trust & Safety - Legal Policy)

Twitter International Company
c/o Trust & Safety - Legal Policy
42 Pearse Street
Dublin 2
Ireland

Fax: 1-415-222-9958 (attn: Trust & Safety - Legal Policy)

Receipt of correspondence by any of these means is for convenience only and does not waive any objections, including the lack of jurisdiction or proper service.

Non-law enforcement requests should be submitted through our Help Center.

Appendix J: Law Enforcement Guide for Snapchat

Accessed 21/07/2015 from
https://www.snapchat.com/static_files/lawenforcement.pdf?version=20150604

Snapchat
Law Enforcement Guide

Last Updated: June 1, 2015

Download the most recent version at: https://www.snapchat.com/lawenforcement

Mailing Address:
Custodian of Records
Snapchat, Inc.
63 Market Street
Venice, CA 90291

Law Enforcement Email for General Inquiries and to Send Legal Process:
lawenforcement@snapchat.com

Law Enforcement Emergency Phone: +1 310-684-3062

I. Snapchat and Law Enforcement

Snapchat is a mobile phone application available through the iPhone App Store and Google Play. The application provides a new way to share moments with photos, videos, and text. The purpose of this guide is to familiarize U.S. law enforcement agencies with the categories of information available from Snapchat and the specific legal process needed to compel that information.

This guide provides information for domestic U.S. governmental and law enforcement agencies. International governmental and law enforcement agencies must rely on the mechanics of the Mutual Legal Assistance Treaty ("MLAT") or letters rogatory to seek user information from Snapchat. Snapchat may provide this guide to international agencies to help them understand how Snapchat works, but the legal process and emergency disclosure provisions apply only to U.S. agencies.

Snapchat is committed to assisting law enforcement investigations as the law requires. That is why we provide not only this guide but also phone and email support to law enforcement agencies for both emergency and non-emergency inquiries. Contact information for Snapchat's law enforcement support is listed on the cover of this guide.

For the most part, Snapchat's ability to disclose user information is governed by the Electronic Communications Privacy Act, 18 U.S.C. § 2701, et seq. ("ECPA"). ECPA mandates that Snapchat disclose certain user information to law enforcement only in response to specific types of legal process, including subpoenas, court orders, and search warrants. Generally speaking, ECPA authorizes law enforcement to compel Snapchat to disclose basic user identity information, login information, and account content (*definitions provided in Section IV of this guide*) in response to appropriate legal process.

It is important to recognize that Snapchat cannot provide legal advice to law enforcement officials. So if you need further clarification about ECPA's restrictions on providers like Snapchat, we suggest that you contact the Department of Justice's Computer Crime and Intellectual Property Section (CCIPS) at 202-514-1026 and ask to speak to the Duty Attorney.

II. How Snapchat Works

Snaps

A user takes a photo or video using their camera phone in real-time. The user then selects a time limit of 1-10 seconds for the receiver to view the photo or video. A user can elect to have the photo/video saved in their phone's photo gallery or just sent via Snapchat, without being saved. The photo/video can then be sent to a friend in Snapchat.

Stories

A user can also add the photo/video Snap to their "Story". Depending on the user's privacy settings, the photos and videos added to a Story can be viewed by either all Snapchatters or just the user's friends for up to 24 hours.

Chat

A user can also type messages to friends within the Snapchat app using the Chat feature. A user sends a Chat message to a friend, and once it is viewed by both parties – and both parties swipe away from the Chat screen – the message will be cleared. Within the Snapchat app itself, a user can opt to save part of the Chat by tapping on the message (text or photo) that he or she wants to keep. The user can clear the message by tapping it again.

III. Locating a Snapchat Account

Before sending a legal request to Snapchat, you must first identify the username of the account. If you are unable to locate a username, Snapchat can try—with varying degrees of success—to locate the account with a phone number or email address.

IV. User Records Maintained by Snapchat and the Legal Process Required to Obtain Those Records

Note: Please send all legal process via email to
lawenforcement@snapchat.com

Snapchat can release user records on a non-emergency basis only if it receives legal process that fully complies with ECPA. The required legal process varies depending on the type of user information you seek:

a. Basic Subscriber Information

Basic subscriber information is collected when a user creates a new Snapchat account, alters information at a later date, or otherwise interacts with the Service. Please note that not all listed information is required, and that user-provided subscriber information is not always independently verified by Snapchat. Basic subscriber information may include:

- Snapchat username
- Email address
- Phone number
- Snapchat account creation date
- Timestamp and IP address of account logins and logouts.

Process required for basic subscriber information: This information can be obtained through a subpoena (including one issued by a grand jury), administrative subpoena, or civil investigative demand pursuant to 18 U.S.C. § 2703(c)(2); a court order issued in accordance with 18 U.S.C. § 2703(d); or a federal or state search warrant.

b. Log of Previous Snaps

Snapchat retains logs of previous messages sent and received. The logs contain meta-data about the messages, but not the content.

Process required for the log of previous Snaps: This information is available pursuant to a court order under 18 U.S.C. § 2703(d) or a federal or state search warrant.

c. Message Content

In certain limited circumstances it may be possible for Snapchat to retrieve the content of sent messages. The reason Snapchat often will not be able to retrieve message content is that Snapchat deletes each Snap from its servers once all recipients have viewed it. And even when a Snap remains unopened, it will be deleted 30 days after it was first sent.

Process required for message content: A federal or state search warrant is required for requests that include message content.

d. International Governmental and Law Enforcement Requests

International governmental and law enforcement agencies must use MLAT or letters rogatory processes to seek user information from Snapchat.

Please note: Snapchat is continuously being updated with new features to improve the user's experience and functionality of the service.

When providing Snapchat with legal process for user records, please provide the following details: the username of the account you seek information from, whether the results must be returned before a specific date, and where the results should be returned.

Snapchat accepts service through email (lawenforcement@snapchat.com) and U.S. mail and overnight courier services (at the address provided on the cover of this guide). Snapchat may produce documents in response to out-of-state domestic legal process such as subpoenas, court orders, emergency requests, and search warrants.

V. Preservation Requests

Snapchat honors requests from law enforcement to preserve information in accordance with 18 U.S.C. § 2703(f). Upon receiving a preservation request on law enforcement department letterhead, Snapchat will preserve

available account information associated with the username listed in the request in an offline file for up to 90 days and will extend the preservation for one additional 90-day period on a renewed request.

Note regarding all legal requests following preservations:
When serving follow-up legal process for information that was previously the subject of a preservation request, please specify whether the request is seeking both the information preserved and any updated user account information. To expedite our response, please also refer to any prior preservation requests by date, or if you received a confirmation email, provide us with the Snapchat case number.

VI. Emergency Requests

Under 18 U.S.C. §§ 2702(b)(8) and 2702(c)(4), Snapchat is able to disclose information voluntarily when we believe in good faith that an emergency posing a threat of death or serious physical injury to any person requires the immediate disclosure of this information.

During non-holiday business hours (Monday to Friday, 9am – 5pm PT), you may request user records on an emergency basis by sending an email to lawenforcement@snapchat.com or by calling 310-684-3062. During non-business hours, you may call 310-684-3062. **Note:** This phone number is for law enforcement emergency requests only. All other law enforcement questions or general inquiries should be sent to lawenforcement@snapchat.com.

All emergency requests must be signed by a sworn law enforcement officer, and those received through email must come from a valid law enforcement email address. Sample Emergency Disclosure form language is provided in section VIII of this Guide. When drafting your emergency disclosure request, please describe the nature of the emergency as specifically as possible and specify the information that you are seeking to resolve the emergency situation.

VII. Snapchat Retention Periods

Snapchat retains different types of user information for different periods of time. Snapchat honors valid law enforcement preservation requests made during the period the requested user information is available.

Basic Subscriber information: The basic subscriber information entered by a user in creating an account is maintained as long as the user has not edited the information or removed the information from the account. Once the user makes a change, the previously existing information is overwritten. Upon receipt of a preservation request, however, Snapchat can capture the user information available at that time; and future actions by the user will not affect the preserved user information. Snapchat also retains logs containing IP addresses associated with account login and logout for a limited period of time after the user has deleted his or her Snapchat account.

Log information. Snapchat retains logs of previous Snaps and may, under certain limited circumstances, store the content of users' unopened Snaps (see the previous discussion of message content in Section IV.C).

VIII. Sample Language and Forms

This section provides sample language that law enforcement may use to complete the section of their legal process identifying the information they seek from Snapchat. These are examples of the most commonly requested information from Snapchat. It is important to be as specific as possible when identifying the information you are requesting from Snapchat.

a. Sample Language for Basic Subscriber Information:
"Records concerning the identity of the user with the username _____ consisting of the email address, phone number, account creation date, and timestamps and IP address for account logins/logouts."

b. Sample Language for Snap Logs

"Logs, including sender, recipient, date, and time, concerning the previous Snaps sent to or from the Snapchat account with the username _____."

c. Sample Preservation Request Letter
(Must be on law enforcement department letterhead and sent from an official governmental email address)

Dear Custodian of Records:

The below listed account is the subject of an ongoing criminal investigation at this agency, and it is requested pursuant to 18 U.S.C. § 2703(f) that the subscriber information associated with said account be preserved pending the issuance of a search warrant or other legal process seeking disclosure of such information:

[Specify username to be preserved].

I understand that Snapchat reserves the right to delete any account that violates its Terms of Use.

If you have any questions concerning this request please contact me at *[insert e-mail address and phone contact]*

Thank you for your assistance in this matter.

Sincerely,

(Your Signature)
(Your Name Typed)
(Your Title Typed)

d. Sample Emergency Disclosure Form
(Must be on the investigating agency or department letterhead and sent from an official governmental email address.)

Dear Custodian of Records:

I request release of records for the Snapchat account associated with _____(username, email address, or phone number) on an emergency basis pursuant to 18 U.S.C. § 2702(b)(8) and § 2702(c)(4).

I have provided below answers to the following questions in enough detail as I am able in order to provide a good-faith basis for releasing records on an emergency basis:

- What is the nature of the emergency involving a danger of death or serious physical injury?
- Whose death or serious physical injury is threatened?
- What specific information in Snapchat's possession related to the emergency are you requesting?

_____ _____

Signature of Sworn Officer Printed Name of Sworn Officer

_____ _____

Agency Date

Appendix K: Law Enforcement Guide for Ask.fm

Accessed 21/07/2015 from http://safety.ask.fm/ask-fm-guide-for-law-enforcement-requests/

Ask.fm Guide For Law Enforcement Requests

1. Background

Ask.fm is an online social network that enables people to send questions to each other and answer them, when they want to. Ask.fm is available as an iPhone or Android application (available through the Apple Store or Google Play), as well as a desktop website. The Ask.fm service provides a way for users to ask each other questions in an anonymous or non-anonymous fashion.

In accordance with our Privacy Policy and Terms of Use Ask.fm Europe Limited ("**Ask.fm**") collects and hosts information created by users and/or concerning user accounts, which may include personal information, when users use its services (collectively '**user data**').

In certain circumstances we may be required by law, or in very limited circumstances we may in good faith believe it is necessary, to provide user data to law enforcement agencies. The purpose of this guide is to inform law enforcement agencies about the way to obtain information from Ask.fm and the specific legal processes necessary to obtain such information. Ask.fm is committed to cooperating with law enforcement investigations to the extent consistent with applicable law. In addition to this guide, law enforcement agencies may also contact Ask.fm with questions or in emergency situations by emailing lawenforcement@ask.fm.

As Ask.fm is an Irish entity and data controller, disclosure of user data is governed by Irish laws, including the Data Protection Acts 1988 and 2003, the Criminal Justice Act 2011 and the Criminal Justice (Withholding of Information on Offences Against Children and Vulnerable Persons) Act 2012. For Ask.fm users in the U.S., U.S. law enforcement only should see section 4, for more information about legal process in the United States arising from the storage of Ask.fm user data in the U.S. Both U.S. and non-U.S. law enforcement requests should be sent to lawenforcement@ask.fm in accordance with sections 6 of this policy.

2. User Data Types

Ask.fm does not respond to law enforcement requests which are overly broad in nature. Furthermore, when cooperating with law enforcement agencies Ask.fm will assess whether the request relates to ***content*** *or* ***non-content*** information.

Ask.fm considers *'**content**'* information as relating to the substantive content of communications (such as user questions and answers); and '***non-content**'* information as relating to basic user information (such as name, registration duration, email address, registration IP address, etc.), as well as to user transactional logs.

Ask.fm collects and stores user information in two ways. This depends on whether a user registers with Ask.fm and is considered a "registered user," or whether a user utilizes

Ask.fm without creating an account or providing any information other than information that is automatically collected as explained in the section below in which case the user is described as a “guest user.”

Information Ask.fm may collect from users includes: name, username, password, email address, postal address, phone number, mobile phone number, payment information, gender, birth year, and other information they provide or post on Ask.fm or allow Ask.fm to access when they do certain things, such as:

- Sign up and complete Ask.fm’s registration form;
- Create or edit user profile;
- Login to the services;
- Submit questions or answer questions;
- Contact our customer support team or use our reporting mechanisms;
- Enter a sweepstakes or contest or register for a promotion;
- Participate in voting or polling activities;
- Request certain features (e.g., newsletters, updates, or other products);
- Connect with the services or otherwise allow us to access certain information about you via a social media service; or
- Post user-generated content to or on our services.

Please note that not all the above mentioned information is required to create an account, and that user-provided information is not always independently verified by Ask.fm.

3. Irish Legal Requirements and Process

A. Mandatory Process

Where Ask.fm receives a mandatory Irish law request, by valid legal process, it may be compelled to produce certain user data it hosts. Absent an emergency, Ask.fm does not disclose user ***content*** information to Irish or non-Irish law enforcement agencies except pursuant to a valid search warrant or court order, which in the case of non-Irish law enforcement requests must be made by first contacting the Central Authority in your country, who will then contact the Office of International Affairs at the U.S. Department of Justice to make a request pursuant to 28 U.S.C. § 1781 *et seq* (the ‘**MLAT**’). The Central Authority in your country may submit the request to:

Office of International Affairs
U.S. Department of Justice
1301 New York Avenue NW, 8th Floor
Washington, DC 20005
Phone (202) 514-0000
Fax (202) 514-0080

Upon service of such valid and mandatory legal process, Ask.fm may be legally compelled to provide ***content and non-content*** user data.

B. Voluntary Cooperation – Non-Mandatory

Where Ask.fm receives requests for ***non-content*** information from Irish or international law enforcement agencies, in the absence of the service of valid and mandatory legal process under Irish law, Ask.fm may in limited circumstances provide ***non-content*** information. This ***non-content*** information may be disclosed where Ask.fm forms a good faith belief that the request is justifiable (under Ask.fm's policies), having assessed it on its merits and taking into account the relevant parts of Ask.fm's Privacy Policy and Terms of Service. In making this assessment, Ask.fm will apply the follow analysis:

- Does the request accord with legal standards in the jurisdiction from which it is made?
- Is the request intended to protect Ask.fm's users or Ask.fm or the public?
- Is the request consistent with internationally recognised norms, such as freedom of speech?

However, except in the case of emergency situations (as described further below), Ask.fm will not disclose ***content*** information in the absence of the service of valid and mandatory legal process, unless otherwise obliged to do so by Irish law.

All voluntary requests for ***non-content*** data from Irish or international law enforcement agencies must comply with the following formalities:

All voluntary law enforcement requests which are ***not*** mandatory disclosures must:

i. be made by a dated request addressed to Ask.fm Europe Limited;
ii. issued on government or official letterhead, or has a caption identifying the court or agency that issued the request;
iii. signed by a judge or other senior official or officer who provides their title and contact information;
iv. in the case of international law enforcement requests, be consistent with the legal requirements of the issuing jurisdiction;
v. be consistent with Irish law;
vi. identify the target, for which information is requested, by providing as much of the following information as possible:
    the account login;
    the account email address;
    the full name of user as registered with Ask.fm; and
    the full URL of the question and answer at issue (e.g. http://ask.fm/askfm/answer/119942892554*)*
vii. specify the types of non-content account information being requested;
viii. specify the legal basis (applicable law) for the request, including the alleged offence (if relevant);
ix. specify why the relevant data is being sought; and
x. specify to whom or how the information being requested is to be delivered.

For the purpose of clarity, this section has no application to U.S.-based demands (see Section 4).

C. Emergency Requests

If law enforcement agencies provide Ask.fm with information that gives us a reasonable good faith belief that there is a risk of imminent harm (i.e. death or serious physical injury) to a person, and that we have information in our possession that may avert that harm, we may disclose the information (***content*** and/or ***non-content***) we have where it is needed urgently to prevent injury or other damage to the health of a person. These requests are assessed by Ask.fm on a case-by-case basis.

Ask.fm may make emergency disclosures of user data to Irish and foreign law enforcement when Ask.fm is provided with facts and circumstances from which it can make a determination that there is:

1. risk of death or serious physical injury to a person or persons;
2. the risk is imminent such that there is not sufficient time to obtain a valid and properly served Irish court order or MLAT order that would normally be required to compel production of user data;
3. the user data requested is relevant to the investigation of the imminent risk; and
4. there is sufficient information for Ask.fm to form a good faith belief that producing the requested user data will assist law enforcement in deterring or otherwise addressing the imminent risk.

All requests for emergency disclosures must be made by law enforcement in the same way set out in sub-section B above **and** we will also need answers to the following questions:

1. What is the nature of the emergency involving death or serious physical injury?
2. Whose death or serious physical injury is threatened?
3. What is the imminent nature of the threat? Please provide information that suggests that there is a specific deadline before which it is necessary to receive the requested information and/or that suggests that there is a specific deadline on which the act indicated in response to Question 1 will occur (e.g., tonight, tomorrow at noon).
4. Please explain/describe how the information you request will assist in averting the threatened death or serious physical injury?

Please send this information via email as a ".pdf" of a letter on official letterhead or via an official government email account to lawenforcement@ask.fm. Please also include your full name, title, rank, badge number, and a confirmation that the information you have provided is complete and accurate.

D. Preservation Requests

We accept requests from law enforcement agencies to preserve records which constitute potentially relevant evidence in criminal proceedings pending the service of valid legal process. Ask.fm will preserve, but not disclose, a one-time temporary snapshot of the then-existing user account record for 90 days pending service of valid legal process. This period may be extended pending an application by a foreign agency via the MLAT process or service of valid and mandatory legal process in the case of Irish law enforcement. Ask.fm will not provide any account data (***content*** or ***non-content***) in these circumstances before

the service of the appropriate legal process. Please send preservation requests to lawenforcement@ask.fm.

4. U.S. Legal Requirements and Process

A. Process Required to Obtain the Records

In order to release account records on a non-emergency basis, Ask.fm requires proper legal process. The legal process required for each type of information is described below in detail.

The legal process submitted to obtain records should include an Ask.fm username, email address associated with the account, the full name of the user (as registered with Ask.fm) and/or the full URL of the question and answer at issue (e.g. http://ask.fm/askfm/answer/119942892554). The request should also indicate if results must be returned before a specific date and where results should be returned.

Ask.fm accepts service of process via email at lawenforcement@ask.fm and will produce documents in response to out of state legal process such as subpoenas, court orders, emergency requests, consent letters and search warrants without requiring domestication.

Subscriber Information and Access Logs

Ask.fm will provide subscriber information and other related transactional information such as access logs in accordance with 18 U.S.C.§ 2703. Ask.fm collects and maintains certain subscriber information when a user creates a new Ask.fm account or alters information at a later date. Please note that not all listed information is required to create an account, and that user-provided information is not always independently verified by Ask.fm. Subscriber information includes:

- fm username;
- Email address;
- Account creation date.

Ask.fm also maintains certain access log data when a user creates an account or accesses their account.
In order to produce such records, Ask.fm requires a subpoena (including grand jury or administrative subpoena) or civil investigative demand pursuant to 18 U.S.C.§ 2703(c)(2), or a court order, search warrant or user consent.

Content Data

Ask.fm maintains user content data and will disclose such data pursuant to proper legal process in accordance with 18 U.S.C. §2703(a) and *United States v. Warshak*, 631 F.3d 266 (6th Cir. 2010).
Ask.fm collects and maintains various forms of content, including images, unanswered questions and answers.

Such content is maintained by Ask.fm as long as the user does not delete such content. A user should not be able to delete content where a preservation request has been previously received by Ask.fm.

In order to produce content information, Ask.fm requires a valid search warrant in accordance with 18 U.S.C. §2703(a).

Preservation Requests

Ask.fm honours requests from law enforcement to preserve information in accordance with 18 U.S.C. § 2703(f). Upon receiving a valid preservation request, Ask.fm will preserve all available account information associated with the username listed in the request in an offline file for 90 days, and an additional 90 days in accordance with a preservation extension request pursuant to 18 U.S.C. § 2703(f) for up to 180 days.

Ask.fm can only preserve information for active accounts. If a request to preserve information is received after an account has been deleted, Ask.fm is not able to honor the request.

Note regarding legal process following preservation requests:

When serving follow up legal process for information that was previously the subject of a preservation request, please specify whether the request is seeking both the information preserved and/or any updated account information. Please also reference any prior preservation requests by date so that Ask.fm may respond to your legal process more efficiently.

In order to preserve information in accordance with 18 U.S.C. § 2703(f), Ask.fm requires a valid preservation request.

B. Emergency Requests

Pursuant to 18 U.S.C. §§ 2702(b)(8) and 2702(c)(4), Ask.fm is permitted to disclose information, including subscriber information and access logs, voluntarily to a federal, state, or local governmental entity when Ask.fm believes in good faith that an emergency involving danger of death or serious physical injury to any person requires such disclosure without delay. Ask.fm will disclose records to assist law enforcement in the case of emergencies meeting the law's threshold requirements.

In accordance with US law, emergency requests from US law enforcement should take the following format:

"Dear Custodian of Records:

I request release of records for username [USERNAME] on an emergency basis pursuant to 18 U.S.C § 2702(b)(7) and § 2702(c). I have provided the answers to the following questions with as much detail as I am able to provide in order to establish a good faith basis for release of records on an emergency basis.

1. What is the nature of the emergency involving death or serious physical injury?
2. Whose death or serious physical injury is threatened?
3. What is the imminent nature of the threat? Please provide information that suggests that there is a specific deadline before which it is necessary to receive the requested information and/or that suggests that there is a specific deadline on which the act indicated in response to Question 1 will occur (e.g. tonight, tomorrow at noon).
4. Please explain/describe how the information you request will assist in averting the threatened death or serious physical injury?

I attest to the truth of the information provided subject to penalty of perjury.

_____ _____
Signature of Officer Printed Name of Law Enforcement Officer

_____ _____
Title and Badge Number Date

Please send this information via email as a ".pdf" of a letter on official letterhead or via an official government email account to lawenforcement@ask.fm. Please remember to include your full name, title, rank and badge number.

C. User Consent

In accordance with 18 U.S.C. § 2703(c)(1)(C), Ask.fm will disclose information based on user consent obtained by law enforcement where sufficient information is provided to verify that the person providing the consent is the actual creator of the account and where law enforcement endorses the authenticity of the consent. Ask.fm will not release information if the user is unable or unwilling to provide registration information that corresponds with the information on record with Ask.fm. In the event that the information provided by the user does not match the information on record with Ask.fm, proper legal process will be required before any information is released.

5. Civil Requests

Ask.fm does not voluntarily respond to requests by lawyers or civil litigants for access to other users' information. Ask.fm will only disclose user data pursuant to valid legal process, except where a request is made with the account holder's explicit consent. This means that Ask.fm will only disclose user information in the context of civil proceedings where we are compelled to do so by a properly domesticated and served subpoena or a court order from a court with jurisdiction over Ask.fm.

Ask.fm has a policy of notifying a user when we receive legal process from a third party requesting that user's data, except in certain circumstances, including where:

- providing notice is prohibited by the legal process itself, by court order we receive, or by applicable law;

- we, in our sole discretion, believe: (a) that providing notice could create a risk of injury or death to an identifiable individual or group of individuals; or (b) that the case involves potential harm to minors. Risk of harm tends to only rarely arise in civil proceedings, therefore Ask.fm will require that the civil party involve law enforcement and that law enforcement communicate this concern to Ask.fm. A civil lawyer's representation regarding a risk of harm in a case without law enforcement involvement will be an insufficient basis on which to withhold user notice.

6. How to Submit Law Enforcement Requests:

In addition to the formalities set out above, all law enforcement requests must:

a) be sent by email to lawenforcement@ask.fm;

b) include in the subject header '*Law Enforcement Request'; and*

c) be in the English language.

7. Policy Changes

This guide may be changed from time to time by Ask.fm, and this document should be consulted in advance of making any law enforcement request.

Ask.fm Europe Limited

Dated February 2015