Considering the Victim: Meeting Victims’ Needs in Relation to Cybercrime and its Impacts

Submission to Public Safety Canada’s Consultation on Cyber Security

Submitted by Sue O'Sullivan, Federal Ombudsman for Victims of Crime
October 2016
Contents

The Office of the Federal Ombudsman for Victims of Crime ................................................... 3
Introduction ................................................................................................................................................... 5
Context ............................................................................................................................................................. 6
  What is cyber victimization? ............................................................................................................. 6
  Cyber victimization vs. “traditional” forms of victimization ......................................................... 7
  Impacts of cyber victimization ...................................................................................................... 8
Key building blocks in addressing cyber victimization ................................................................. 10
  Collection of data and statistics ................................................................................................ 10
  Raising public awareness & training .......................................................................................... 14
  Supports for victims ...................................................................................................................... 16
  Cross-sectoral partnerships ........................................................................................................ 18
  Legislation ........................................................................................................................................... 19
Conclusion ................................................................................................................................................... 23
Summary of recommendations .......................................................................................................... 24
Sources .......................................................................................................................................................... 25
The Office of the Federal Ombudsman for Victims of Crime

The Office of the Federal Ombudsman for Victims of Crime (OFOVC) is an independent resource for victims in Canada. It was created in 2007 to ensure that the federal government meets its responsibilities to victims of crime.

Our mandate relates exclusively to matters of federal jurisdiction and enables us to:

- promote access by victims to existing federal programs and services for victims;
- address complaints of victims about compliance with the provisions of the Corrections and Conditional Release Act that apply to victims of crimes committed by offenders under federal jurisdiction;
- promote awareness of the needs and concerns of victims and the applicable laws that benefit victims of crime, including to promote the principles set out in the Canadian Statement of Basic Principles of Justice for Victims of Crime with respect to matters of federal jurisdiction, among criminal justice personnel and policy makers;
- identify and review emerging and systemic issues, including those issues related to programs and services provided or administered by the Department of Justice Canada or the Department of Public Safety and Emergency Preparedness Canada, that impact negatively on victims of crime; and
- facilitate access by victims to existing federal programs and services by providing them with information and referrals.

We are also involved in ongoing discussions with the Government about our mandate in relation to the Canadian Victims Bill of Rights (CVBR). The CVBR gives registered victims of crime a more effective voice in the criminal justice system, providing statutory rights for victims with respect to information, protection, participation, and restitution, as well as providing victims with the right to remedies.¹

¹ Victims who believe that any of their rights under the CVBR have been infringed or denied by a federal entity have the right to file a complaint.
An important part of the OFOVC’s work is to amplify the voice of victims of crime in Canada, which means ensuring that victims are *informed, considered, protected,* and *supported.* As such, we welcome the opportunity to provide input to Public Safety Canada’s Cyber Consultation.
Introduction

Every day, Canadians are victimized online. Such victimization takes many forms and can give rise to serious and enduring impacts on the individuals it harms and their loved ones.

Based on listening to the perspectives of victims, victim-serving agencies, and related experts on cybercrime and cyber victimization, it is our perspective that a victims’ lens must be applied in the development of Canada’s renewed approach to cyber security. In order to address such issues as prevention or deterrence, we must work backwards to determine what it is specifically that we are aiming to prevent. A broad approach to ensuring healthy and safe communities would suggest that prevention is required not only in relation to the commission of the crime itself, but also in relation to its lasting impacts and any further harm or traumatization a victim may suffer as a result of their journey through the criminal justice process. Where we are aiming to minimize harm and maximize resiliency in the aftermath of a crime, we must be prepared to consider, upfront, the needs and concerns of victims of crime and to address and prioritize those needs and concerns in the development of any programs, policies, legislation, and strategies. Having victims’ perspectives at the forefront of the conversation will also help to ensure that their rights and needs are being respected, that they have access to appropriate supports and services, and that they feel empowered to report cybercrime and to act as engaged participants in the criminal justice system.

To that end, this submission provides context on cyber victimization and why it matters within the broader cyber security framework. It also presents recommendations across five “building block” areas pertaining to cyber victimization. These include data and statistics, public awareness and training, victim-centred supports, cross-sectoral partnerships, and legislation.

---

2 Cyber victimization includes a mix of incidents that are currently criminal offences under the *Criminal Code* and others that are not.
Context

What is cyber victimization?

When looking at cyber security and cyber threats, ultimately we want to avoid victimization and its subsequent impacts. Cyber victimization takes many forms. Some examples include cyberbullying,\(^3\) cyber stalking and harassment, Internet bank and credit card fraud, and identity theft.

As well, both younger Canadians—including children—and adults are victimized by cyber sexual violence, which can take many forms. One example is the distribution of sexual recordings, images, or messages without consent. In some cases, the distributed image is of a sexual assault, whereas in other cases, it depicts consensual sexual acts. This can also include “revenge porn,” which refers to the sharing of intimate images online without the consent of an individual, most frequently by a former romantic partner seeking to humiliate and harm them. Other types of cyber sexual violence include the online luring and online sexual exploitation of minors by adults who are communicating with them for the purpose of committing a sexual offence; “sextortion,” through which victims are threatened with the online distribution of sexual images or information, sometimes with the additional caveat that the victims can “prevent” the distribution of this material if they undertake certain sexual or illegal activities; and virtual sexual assault, whereby a victim receives online threats of sexual assault from one or more individuals.

Given the evolving nature of the online environment, other forms of victimization are also emerging. For example, there is growing awareness of use of the Internet to recruit potential victims of human trafficking or to lure them to a particular location in order to rob them.

---

\(^3\) Cyberbullying “involves the use of communication technologies such as the Intranet, social networking sites, websites, email, text messaging and instant messaging to repeatedly intimidate or harass others.” It can involve, for example, sending threatening emails, text messages, or instant messages, or tricking someone into revealing personal or embarrassing information and sending it to others. [http://www.rcmp-grc.gc.ca/cycp-cpcj/bull-inti/index-eng.htm](http://www.rcmp-grc.gc.ca/cycp-cpcj/bull-inti/index-eng.htm)
Cyber victimization vs. “traditional” forms of victimization

Cybercrime changes the traditional dynamics between offenders and victims. Researchers have identified unique features of the online environment which differentiate cyber victimization from traditional forms of victimization. These include:

- **Increased accessibility**—Whereas predators may have traditionally required in-person or proximity access to victims, they are now able to log on and access thousands, if not millions of victims at any given time. The areas of access are also far more vast. For example, where sexual predators may have once had to rely on relatively few forums (schools, sports, etc.) the platforms by which they can reach out to victims are far more numerous and include things like chat rooms, gaming platforms, social media and more. The online world is not bound by typical time constraints; harm can be inflicted 24 hours a day, 7 days a week.

- **Anonymity or disguise**—victimization can be carried out on a global scale, while those perpetrating it remain in relative anonymity. Given this anonymity, perpetrators may also find it easier to be cruel since they cannot see or be seen by their victims. That anonymity may also enable predators to disguise themselves, posing as persons of the opposite gender or a younger age, which may encourage children to be more open and trusting when sharing information or arranging to meet.

- **Detectability**—Where traditional theft or assault leaves physical traces, in some cyber cases, victims may not even be aware that they have been victimized for some time. These could include cases where someone’s sexual images are being shared over the Internet without their consent, or where victims have experienced financial theft.

---

• **Rapidity and inability to constrain**—Images can be shared with astonishing speed and, unfortunately, are often impossible to completely trace and remove. Cruel comments can flood a website in minutes, and identity theft or financial scams can result from replying to just one phishing email.

These and other factors, coupled with the complex, evolving nature of the online world, contribute to making cyber victimization particularly difficult to predict, prevent, investigate, or prosecute.

**Impacts of cyber victimization**

Although cybercrime is sometimes viewed as remote, intangible, or even “victimless,” the victimization and the associated impacts are real and substantial.

The International Centre for Criminal Law Reform and Criminal Justice Policy acknowledged identity crime as “one of the fastest growing and most serious economic crimes in North America.” In 2013, the Canadian Anti-Fraud Centre reported over $52 million lost due to mass marketing fraud and approximately $11 million lost due to identity fraud. In 2014, police-reported cybercrime in Canada included serious crimes such as criminal harassment, child pornography, uttering threats, sexual exploitation, and luring a child. Furthermore, identity fraud and child pornography—two crimes now generally associated with the use of the Internet and information technologies—were among the few police-reported crimes that increased in both volume and severity between 2013 and 2014.

It is important to remember that cybercrime is not a victimless crime. As with other forms of victimization, it has harmful impacts. Victims of cyber-based identity fraud, for example, can experience a range of harms, such as direct financial loss (goods, services, or cash lost to the person who misused the victim’s account or personal

---

6 Statistics Canada, 2016, Police-reported data on hate crime and cybercrime, 2014: Police-reported cybercrime, by most serious violation, Canada.
information), harassment by creditors or debt collectors, lost income and/or 
economic opportunities due to a tarnished financial reputation (e.g., inability to 
access credit due to fraud or corrupted identity, or loss of employment), loss of 
family and social trust as a result of a damaged reputation, trauma, and depression.\(^8\)

Another example of cybercrime with dire impacts is cyber sexual violence. For 
example, young victims of cyber sexual violence may be relentlessly bullied and 
harassed not only by the offender but also by their peers, which can cause mental 
health issues such as anxiety or depression or even result in suicide. In addition to 
the short-term impacts of cyber sexual violence, relatively little is known about the 
long-term impacts. For victims of all ages, knowing that the images of their abuse 
continue to be in circulation can be extremely traumatic. Some victims have gone so 
far as to say that the enduring trauma of knowing those images are out there was 
worse than the abuse itself. Despite this, little research has been done to date on 
these unique types of trauma and how we can best support these victims of crime.

These are but a few examples of the negative impacts of cyber victimization on both 
society and individuals. They highlight the importance of assisting and supporting 
victims to prevent ongoing victimization and to mitigate the effects of cybercrime.

\(^8\) Ibid. and C. Cross, 2016, I’m Anonymous, I’m a voice at the end of the phone: A Canadian case study into the 
Key building blocks in addressing cyber victimization

In order to properly evaluate, consider, and address the needs of Canadians who have been, or may be, victimized through cyber technology, the OFOVC recommends that the Government of Canada consider the following key “building block” components when developing its strategies or policies, and that it address the recommendations provided.

Collection of data and statistics

**Recommendation 1:** Enhance, regularize, and standardize data collection on cyber victimization in Canada, and consider introducing a new national survey specific to cybercrime and cyber victimization and/or a centralized reporting database.

Cyber victimization is difficult to measure and quantify. Based on results from the Uniform Crime Reporting (UCR) survey, according to Statistics Canada, in 2014, 15,187 incidents of cybercrime were reported to the police, with fraud, child pornography, and uttering threats among the most reported serious crimes. However, such data represent just the tip of the iceberg and are an under-representation of the full extent of cyber victimization, due to a number of factors, such as non-reporting by victims and/or reporting to authorities other than the police.

- **Non-reporting by victims**—Victims may be unwilling to acknowledge that they have been victimized due to embarrassment (e.g., a victim may feel embarrassed that they provided personal information to someone who sought to harm them) or uncertainty about what to do (e.g., whether or not the crime should be reported and, if so, to whom). They may also fear that they will not be believed or will be blamed—a fear that is reinforced when other victims who report their experiences are met with responses such as

---

9 Incidents reported to selected police services that report to the most recent version of the Uniform Crime Reporting (UCR) Survey (Statistics Canada), which is designed to measure the incidence of crime in Canadian society and its characteristics. UCR data reflect reported crime that have been substantiated by police.


“just stay off the Internet.” Furthermore, some time may elapse before individuals realize that they have been victimized, at which point they may decide it is pointless to report the incident to the police. In the case of youth, they may also be concerned that reporting will lead to increased scrutiny or oversight of their online activities.

- **Reporting to other authorities**—Even when cyber victimization is reported, the reporting does not always flow through a single portal, such as police, in the same way as information about traditional crimes might. For example, a victim of credit card fraud might only report the incident to their bank and not the police, or a youth who feels they are being bullied may contact a social media site or a teacher for help.

Due to these and other factors, such as a lack of timely data collection across the entire spectrum of types of cyber victimization, the full extent of cybercrime and cyber victimization in Canada is currently unknown. In order to better understand the nuances and scope of the problem, and to be able to develop appropriate responses, Canada needs regular, consistent, comprehensive metrics on cyber victimization. Collecting data on cyber victimization through surveys with Canadians, on a regular basis, would yield a clearer, more up-to-date, and richer picture of the problems underlying cyber security issues in Canada. The information would not only serve to deepen our understanding of the experiences of cyber victims in order to be able to provide them with appropriate responses, but also enhance our capacity to develop evidence-based policies, programs, and laws, more broadly.

Currently, in addition to data on police-reported cybercrime collected through the UCR, Statistics Canada collects data on some elements of cyber victimization through the Canadian Internet Use Survey. These data pertain to Canadians’ experiences in relation to misuse of personal information on the Internet and email requests for personal financial information received from a fraudulent source.

---


13 The Canadian Internet Use Survey is a hybrid survey that measures both household Internet access and the individual online behaviours of individual household members.
Statistics Canada also collects data on Internet-based victimization as part of its General Social Survey (GSS) on Victimization. The GSS on Victimization asks Canadians about their experiences with several types of victimization, including both crime incidents that are reported to the police and those that are unreported (i.e. self-reported incidents). Since many crimes are not reported to police services for a variety of reasons, self-reported victimization data, such as those provided by the GSS, provide an essential complement to justice system statistics.

A major challenge is that the GSS on Victimization is repeated only every five years, with the most recent survey issued in 2014, which does not permit access to up-to-date statistics on cyber victimization to keep pace with the evolving nature of such victimization. Another challenge is that neither the Canadian Internet Use Survey nor the GSS on Victimization collects data on a comprehensive range of cyber victimization experiences. For example, the 2014 GSS on Victimization included questions only in relation to cyberbullying and cyber stalking. It did not retain questions pertaining to cyber victimization that were introduced in the survey, for the first time, in 2009. The 2009 survey included special modules which collected useful information from Canadians about their perceptions and experiences of Internet victimization in relation to cyberbullying, child luring, Internet bank fraud, problems encountered with making online purchases, and “phishing” in the form of receiving fraudulent email from someone posing as a legitimate organization requesting personal information. The next GSS on Victimization cycle will be in 2019, and content development is currently under way. The timing could provide an opportunity to add additional content in order to better address data gaps related to cyber victimization, including, for example, questions pertaining to cyber sexual violence, such as revenge porn.

Given that the GSS on Victimization is only conducted every five years and may not be the optimal tool for assessing the frequency and impact of cyber victimization, it is the OFOVC’s perspective that a new, separate survey on cybercrime and cyber

---

14 The target population is Canadians aged 15 and over. The GSS on Victimization is the only national survey of self-reported victimization which provides data for the provinces and territories, including by conducting interviews in Canada’s north.

15 The GSS is conducted on six different themes (caregiving, families, time use, social identity, volunteering, and victimization), with each theme repeated in depth every five years.

16 The GSS asked respondents aged 15 and over about their personal experiences with cyberbullying. It also asked respondents aged 18 and over with children aged 8 to 17 living in their household about the children’s experiences with cyberbullying.
victimization, built in collaboration with the provinces and territories, is warranted. A stand-alone survey would permit opportunities for regular content updates to keep pace with the evolving nature of cyber victimization. It would also allow for inclusion of questions relating to a broader range of types of cyber victimization, as well as for a more comprehensive exploration of the issues, for example by including questions on victims’ outcomes in relation to the cyber victimization (e.g., whether they accessed services, types of supports received, self-reported degree of harm experienced). Similar to the GSS on Victimization, any such survey would need to retain a focus on self-reported incidents, in order to ensure that the experiences of victims who do not report are captured.

To that end, Canada could strive to develop a system such as the Australian Cybercrime Online Reporting Network (ACORN). ACORN is a national database that was designed in collaboration with police, businesses, Australia’s national statistical agency, and the Government of Australia. It allows for reporting and information sharing on a full spectrum of various types of cybercrime, such as online scams or fraud, online identity theft, cyber bullying, sexting, online harassment or stalking, and online child abuse or child sexual abuse material. Data can be entered by police, credit card companies, individual victims of cybercrime, businesses that have received cyber attacks or threats, and Australia’s Cyber Security Department. Australia’s National Statistical Agency can access the data without seeing personal information to produce quarterly reports on the volume of cybercrime, as well as on key trends, positioning the Government to have better information on cybercrime and cyber security threats. Police can access it for intelligence purposes to investigate offences or look for patterns. Credit card companies and banks can use the data for insurance purposes, as well as to recover losses, and businesses can access the data to better protect themselves. ACORN was presented at the 2016 annual meeting of the Canadian Association of Chiefs of Police as a promising practice.

Ultimately, having reliable statistics on cyber victimization will largely depend on having a full complement of cyber victimization data, not only from police-based reporting and self-report victimization surveys, but also from other sources such as the Canadian Anti-Fraud Centre (the central agency in Canada that collects information and criminal intelligence on such matters as mass marketing fraud, advance fee fraud, Internet fraud, and identity theft) and the Canadian Centre for
Child Protection (which operates Canada’s national tip line for reporting the sexual exploitation of children). Efforts to standardize common definitions of various forms of cybercrime and cyber victimization across the various data collection tools and to collaborate on creating more seamless, integrated data capture and data sharing processes, to the extent possible, would also help to yield a more accurate picture of cyber victimization in Canada.

Raising public awareness & training

**Recommendation 2:** Increase public awareness of cyber-based victimization, and ensure that criminal justice system personnel have adequate training on cyber victimization.

Public campaigns and education curricula can greatly influence societal perceptions of acceptable behaviour and can be effective tools to help the public recognize cyber-based victimization. Activities in cyberspace seem to be challenging societal understanding of criminal versus non-criminal behaviour. Many people do not recognize the harm associated with cyber-based criminal victimization and/or do not see its harm as being on par with other forms of criminal victimization. A broad public dialogue is needed to:

- address the lack of cybercrime awareness among the general population,
- enhance understanding that crime committed online is crime,
- raise awareness of the serious impacts on victims,
- encourage reporting both by victims and others,
- counter the current phenomenon of victim-blaming that many victims of Internet victimization experience, and
- improve digital literacy as it relates to privacy, safety, and how we interact with one another online.

This dialogue must include *all* Canadians, and not merely young Canadians and their parents.

---

Awareness-raising efforts should include initiatives centered on increasing sensitivity to the gendered nature of cyber victimization. For example, while anyone can be a victim of cyberviolence, the majority of victims of cyberviolence, particularly cyber sexual violence, are young women and girls. In 2012, police identified 2,070 victims of violent cybercrime; females accounted for 69 percent of victims of violent cybercrime, including 84 percent of victims of sexual violations. An example of a promising initiative that raises awareness of the gendered nature of cyber victimization is Project Shift, a YWCA Canada project funded by Status of Women Canada. Its goal is to create a safer digital world for girls and young women. In support of this objective, Project Shift has conducted a needs assessment study, with a focus on identifying the gender-specific issues regarding cyberviolence. Project Shift has been sharing the findings of the study to garner support for the strategies developed in response to the recommendations resulting from the needs assessment. The aim is to create systemic change that will promote a gendered lens in understanding and responding to cyberviolence. Assessing and understanding the online safety needs of girls and young women through initiatives such as Project Shift will ultimately help create better supports for victims of cyberviolence.

While global awareness is important, it is also crucial that key participants in the criminal justice system be trained to respond to victims in an appropriate manner. This would include being aware of the types of supports a cybercrime victim may need and providing those supports in a considerate and non-judgmental manner.

---

Supports for victims

**Recommendation 3:** Ensure that victim-centred supports are available for those who have experienced cyber victimization.

Approaches to tackling cybercrime should include a focus on victim-centred support services that address the unique circumstances of technology-facilitated victimization. The type of support that victims of cybercrime may need can range from very basic services, such as providing an interim phone or computer while the victim’s items are in police possession for forensic investigation, or more critical services, such as implementing a peace bond or specialized counselling for women who have experienced violent threats online. Victims may also need guidance on how to restore their financial and/or personal reputation, advice on how to protect themselves from further victimization, referrals to suitable professional services specialized in helping cybercrime victims, and information about their rights and about the investigation and prosecution of their complaint.

As with all victims, it is important to recognize that cyber victims may also have a need not only for immediate supports, but also for supports over a longer period. To that end, the Canadian Centre for Child Protection is currently undertaking an international survey of the first generation of survivors of online sexual exploitation, aimed at providing a more nuanced insight into how online child sexual exploitation affects victims long term. Recommendations on how to better support victims will be forthcoming. Initiatives such as these that bring victims’ voices to the table are critical to our understanding, as it is victims themselves who have the best insight into the types of supports that may be needed, as well as any existing gaps.

---

19 Ibid. at 5.
20 Ibid.
In addition to practical supports, legislative supports and enshrined rights are also important in a victim-centred approach. While the specific circumstances and needs of each victim vary, the Canadian Victims Bill of Rights\(^{21}\) provides all victims of crime, defined as individuals “who ha[ve] suffered physical or emotional harm, property damage or economic loss as the result of the commission or alleged commission of an offence,” in Canada with certain statutory rights.\(^{22}\) Moving forward, addressing cybercrime will necessarily require that its victims receive justice and are able to exercise their rights as provided for in the CVBR, which are as follows:

- **Right to information**—Victims have a right to request general information about the criminal justice system and available victim services and programs. They also have the right to request specific information relating to the investigation, prosecution, sentencing, and conditional release of the person(s) who harmed them.

- **Right to protection**—Victims have a right to have their security and privacy considered at all stages of the criminal justice process, and for reasonable and necessary measures to be taken to protect them from intimidation and retaliation. As well, they have the right to request that their identity be protected from public disclosure, and to request to use testimonial aids when appearing as a witness.

- **Right to participation**—Victims have a right to convey their views about decisions to be made that affect their rights under the CVBR, and to have their rights considered at various stages of the criminal justice process. Victims also have a right to present a victim impact statement to the court or Review Board, and to have it considered.

\(^{21}\) The Victims Bill of Rights: An Act to Enact the Canadian Victims Bill of Rights and to Amend Certain Acts created the legislative recognition of victims’ rights and made amendments to the Criminal Code, Corrections and Conditional Release Act, Canada Evidence Act, and Employment Insurance Act. While most of the provisions came into force on July 23, 2015, others were implemented more recently, on June 1, 2016. [http://www.parl.gc.ca/content/hoc/Bills/412/Government/C-32/C-32_4/C-32_4.PDF](http://www.parl.gc.ca/content/hoc/Bills/412/Government/C-32/C-32_4/C-32_4.PDF)

\(^{22}\) As per subsections 18(1) and (2) of the CVBR, the rights apply to a victim of an offence in their interactions with the criminal justice system while the offence is reported, investigated or prosecuted; the offender is subject to the corrections process or the conditional release process; and the accused is under the jurisdiction of a court or Review Board, if they are found not criminally responsible on account of mental disorder or unfit to stand trial.
• **Right to seek restitution**—Victims have a right to have the court consider making a restitution order against the offender. As well, every victim with a restitution order has the right, if they are not paid, to have the order entered as a civil court judgment that is enforceable against the offender.

• **Right to file a complaint**—Any victim who is of the opinion that any of their rights under the CVBR have been infringed or denied by a federal department/agency also has the right to file a complaint in accordance with the federal entity’s complaints mechanism. Further, any victim who has exhausted his or her recourse under the complaints mechanism, and who is dissatisfied with the outcome, may file a complaint with any authority that has jurisdiction to review complaints in relation to that federal entity, such as the OFOVC.

Cross-sectoral partnerships

**Recommendation 4:** Enhance collaborative partnerships across sectors.

Current research suggests that solutions to cyber victimization demand effective collaboration amongst multiple partners—youth and youth leaders, parents, educators, researchers and academia, law enforcement, industry (e.g., Internet service providers, mobile phone companies, social networking and online gaming sites, software developers, etc.), non-government organizations, the private sector, and communities. It will take comprehensive effort from all partners to make a difference in preventing and addressing cyber victimization.

Law enforcement will also need to be nimble in their approach as cybercrime often occurs across provincial/territorial and national boundaries. Police-reported data indicate that the jurisdiction where the offence is reported is not necessarily where the victimization occurred. Therefore, coordination across federal and provincial/territorial policing jurisdictions is required even though the resources and activities devoted to cybercrime may vary from one jurisdiction to another.\(^\text{23}\)

---

An example of a coordinated approach at the provincial level is Ontario’s *Provincial Strategy to Protect Children from Sexual Abuse and Exploitation on the Internet*. The Ontario Provincial Police, the Ontario Association of Chiefs of Police, the Ministry of Community Safety and Correctional Services, and the Ministry of the Attorney General implemented a multi-disciplinary, province-wide approach to fight online child exploitation crimes. The approach ensures that police and Crown prosecutors are trained on the unique circumstances of investigating and prosecuting cyber sexual crime, and that specialized counselling is available for victims. The goal is to “effectively address the ‘complete picture’ of child sexual abuse and exploitation—from the outset of an investigation, to offender apprehension and management, effective prosecution and sentencing, victim identification and support, as well as prevention and awareness.”

**Recommendation 5**: Ensure that Canadians are informed about existing laws, and address key legislative gaps regarding online child sexual and physical abuse images.

Legislation to address cybercrime requires regular evaluation and updating to ensure that effective legal remedies exist, and to address any gaps. Given the vulnerability of children and Canada’s obligation to protect them from abuse, it is the OFOVC’s perspective that priority should be placed on addressing gaps in relation to online child sexual exploitation and abuse, and online child physical abuse images.

*Online child sexual exploitation and abuse*

The Government of Canada, along with some provincial governments, has enacted legislation requiring individuals to report possible child pornography content. The goal of mandatory reporting is to facilitate the removal of child pornography from the Internet, thus reducing the circulation of sexual abuse images, supporting

---

victims, and identifying those committing crimes against children. Furthermore, enacted in March 2015, the Protecting Canadians from Online Crime Act allows for criminal prosecutions when sexual pictures are shared without consent and when there was a reasonable expectation the images would be kept private.

While legislation is in place to address some forms of online sexual exploitation, there may be a need for enhancements over time. Sexual cyber victimization can be carried out in many forms, some of which may not be fully addressed under criminal law. Images that depict the sexual commodification of children, such as images or videos of sexualized child modelling are one example. Such images may serve to normalize or promote harm to children, while also signalling children who are in danger, yet they can escape criminal investigation and/or prosecution. In her testimony to the House of Commons Standing Committee on the Status of Women regarding violence against young women and girls in Canada, the Executive Director of the Canadian Centre for Child Protection stated that “[w]hile the current definition of child pornography in Canada is broad enough to capture the most egregious of sexualized child modelling pictures under the Criminal Code definition, the majority would fall outside of it.”

In addition to addressing gaps in legislation, it is also necessary to ensure that criminal justice staff are aware of current cybercrime legislation. Testimony provided to the House of Commons Standing Committee on the Status of Women regarding violence against young women and girls in Canada highlighted the variability in awareness and competency, among criminal justice staff, in dealing with cyber-based victimization. Examples were provided of young women reporting to police about their sexual images being shared online only to be misinformed that there is no legal remedy. This disconnect reinforces the importance of public awareness and training of criminal justice staff, more broadly.

Online child physical abuse images

Another example of a current legislative loophole relates to online child physical abuse images. While the *Criminal Code* contains provisions to address most forms of child pornography, there are no complementary provisions that prohibit the recording and the sharing or posting of child physical abuse images on the Internet, or that compel removal of such images from Internet content networks (e.g., Facebook, Twitter, YouTube, etc.). In recognition of this gap, in August 2016, the Canadian Association of Chiefs of Police passed a resolution aimed at addressing the proliferation of online material depicting the physical abuse of children. Given that “child abuse imagery violates the dignity, rights and privacy of a victimized child and also signals that there is likely a child in dire need of protection,” the resolution “urge[s] the Government of Canada to protect children by amending the *Criminal Code* to prohibit the making and posting of child abuse imagery as well as mandating the removal and deletion of such images from the Internet.”

As noted by the Association:

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

The OFOVC is likewise concerned with the current lack of laws to address online child physical abuse imagery. The result is that there is no mechanism to enable the investigation and arrest of those who victimize people by posting child abuse images online, to facilitate protection of child abuse victims from ongoing harm, or to compel removal of the images from the Internet. At present, it is left to content providers to determine whether and how to take action (e.g., remove the images, block the user, etc.), according to their internal policies. Moreover, content providers are exempt from having to provide the necessary information to law enforcement.

---

28 Ibid. (CACP Resolution #02-2016 Child Physical Abuse Imagery).
enforcement. As with child pornography, legislation must be in place to prevent the harm caused both to the child and to the public by the posting and spreading of child physical abuse imagery. Having such images recorded and distributed on the Internet re-victimizes child victims, can traumatize those who view them, and serves to normalize—or, worse, promote—child abuse. It is therefore the OFOVC’s perspective that amendments to legislation are needed to protect both victims and the public.
Conclusion

In the development of any response to the cyber security challenges that face us, it is essential that Canada consider the victims. How can we better prevent victimization? How do these crimes impact victims in the short, medium and long term? What will be the victims’ experience with the criminal justice system, and how we can best respond to their needs and concerns?

An effective response will need to be underpinned and informed by data and research; therefore, regular data collection and analysis is an important building block. An effective response will also require a conversation that draws in all Canadians in order to shift societal attitudes and to bring awareness not only to the potential for victimization, but also to the needs of victims in the aftermath of a crime. Hand-in-hand with awareness comes training and sensitization for those working with victims within the criminal justice system, so that they can better understand, and address, the unique needs of cyber victims. While prevention is the goal, victim-centred responses must be in place to address the harm done to those who have been affected by the many different types of cyber-based victimization. Those responses must be developed, and initiated, across sectors. Victims—including youth victims—and victim-serving agencies have a specific and important expertise to contribute to the conversation, and their input should help to inform decision-making with respect to policy, programs, and legislation. Finally, the legislation in place must reflect the realities both of a fast-paced technological environment and of the unique needs and concerns of victims of crime. We must ensure that Canada’s laws protect children and send a clear message that any form of child abuse or sexual commodification is simply unacceptable.

In conclusion, the OFOVC respectfully submits its recommendations to the Government of Canada and welcomes the opportunity to be part of this important dialogue moving forward.
Summary of recommendations

- **Recommendation 1:** Enhance, regularize, and standardize data collection on cyber victimization in Canada, and consider introducing a new national survey specific to cybercrime and cyber victimization and/or a centralized reporting database.

- **Recommendation 2:** Increase public awareness of cyber-based victimization, and ensure that criminal justice system personnel have adequate training on cyber victimization.

- **Recommendation 3:** Ensure that victim-centred supports are available for those who have experienced cyber victimization.

- **Recommendation 4:** Enhance collaborative partnerships across sectors.

- **Recommendation 5:** Ensure that Canadians are informed about existing laws, and address key legislative gaps regarding online child sexual and physical abuse images.
Sources

http://www.parl.gc.ca/content/hoc/Committee/421/FEWO/Evidence/EV8452214/FEWOEV23-E.PDF

http://www.parl.gc.ca/content/hoc/Committee/421/FEWO/Evidence/EV8437884/FEWOEV22-E.PDF


