Report on the Review of the Intimate Images and Cyber-protection Act

NOVA SCOTIA

Report on the Review of the Intimate Images and Cyber-protection Act

ISBN 978-1-77448-400-5

Contents

Executive Summary

The Nova Scotia Department of Justice ("Department of Justice") has completed a review of the *Intimate Images and Cyber-protection Act* ("*IICPA*" or "the *Act*") on behalf of the Minister of Justice, pursuant to Section 14 of the *Act*. The objectives of the review were to assess the effectiveness of the *IICPA* in achieving its purpose and outline recommendations.

The stated goals of the *IICPA* are to:

- discourage, prevent, and respond to the harms of non-consensual sharing of intimate images and cyberbullying;
- uphold and protect the fundamental freedoms of thought, belief, opinion, and expression, including freedom of the press and communication media; and
- help Nova Scotians respond to non-consensual sharing of intimate images and cyberbullying.

The *IICPA* was enacted in July 2018, allowing victims of cyberbullying and/or non-consensual intimate image distribution to initiate a voluntary court process for private legal disputes. The *Act* designates the CyberScan unit at the Department of Justice to:

- provide public information and education regarding harmful on-line conduct;
- advise public bodies on policies for online safety and conduct;
- provide support and assistance to victims of intimate image distribution without consent and cyberbullying;
- provide information to victims of intimate image distribution without consent and cyberbullying respecting the criminal justice system and proceedings under the *Act*;
- provide information to victims of intimate image distribution without consent and cyberbullying about contacting police;
- provide voluntary dispute-resolution services, including advice, negotiation, mediation, and restorative justice approaches in respect of harmful on-line conduct; and
- provide such other services, exercise such other powers and authorities, and perform such other duties as may be prescribed by the regulations.

Evoke Consulting was hired to design a trauma-informed public consultation process with the Department of Justice. It was decided that interactive sessions would be offered throughout the province to learn from stakeholders' experiences and feedback in connection with the *Act*. The consultation was launched in January 2022, incorporating trauma-informed approaches due to the sensitive nature of non-consensual intimate image sharing and cyberbullying. Engagement sessions were inclusive by design and prioritized outreach to diverse stakeholders across Nova Scotia.

The objectives of the public consultation were to:

- deepen the understanding of the public/stakeholders' lived experiences related to the *IICPA* and its delivery;
- uncover stakeholder observations, challenges, and needs; and
- identify opportunities to improve upon the *Act* and its implementation.

Over 460 Nova Scotians engaged in the consultation through a variety of methods:

11 small group sessions (59 participants)

- Indigenous, African Nova Scotian, and Acadian/francophone community members;
- law enforcement;
- youth;
- persons with disabilities; and
- education stakeholders.

8 individual conversations (8 participants)

- victims; and
- legal and academic professionals.

An anonymous online survey (399 participants)

- victims;
- professionals;
- public with no direct experience;
- victims;
- family members/friends/partners;
- parents/guardians;
- preferred not to say; and
- other.

This report is a synthesis of the perspectives shared by public consultation participants and stakeholders across Nova Scotia.

Background

2.1. Cyber-safety Act

In 2013, Nova Scotia passed the *Cyber-safety Act* ("*CSA*") becoming the first jurisdiction in Canada to address cyberbullying and the dangers of social media in civil legislation (Dinning, 2013). The *CSA* provided a broad definition of cyberbullying that included both adults and minors (individuals less than 19 years of age). Under section 3(1)(b) of the *CSA*, cyberbullying was defined as:

"[A]ny electronic communication through the use of technology including, without limiting the generality of the foregoing, computers, other electronic devices, social networks, text messaging, instant messaging, websites and electronic mail, typically repeated or with continuing effect, that is intended or ought reasonably be expected to cause fear, intimidation, humiliation, distress or other damage or harm to another person's health, emotional well-being, self-esteem or reputation, and includes assisting or encouraging such communication in any way."

The *CSA* created both civil law and informal remedies for cases of cyberbullying. It established a tort (a civil, non-criminal legal liability for cyberbullying) which gave the Court the option to award financial compensation to the victim. The *CSA* set out a procedure for complainants to apply for a Cyberbullying Prevention Order from the Supreme Court of Nova Scotia. If granted, the Court could:

- prohibit the bully from engaging in cyberbullying;
- restrict or prohibit the bully from, directly or indirectly, communicating with or contacting the victim or any other specified person;
- restrict or prohibit the bully from, directly or indirectly, communicating about the victim or any other specified person;
- prohibit or restrict the bully from using electronic communication;
- confiscate, for a specified period or permanently, any electronic device capable of connecting to an Internet Protocol (IP) address associated with the bully or used by the bully for cyberbullying;
- require the bully to discontinue receiving service from an internet service provider; or
- take any other measure considered necessary or advisable for the protection of the victim.

In addition, the *CSA* established the CyberScan unit within the Department of Justice, to investigate cyberbullying complaints and negotiate resolutions between accused bullies and victims. Under the *CSA*, CyberScan staff had the authority to:

- apply for court orders requiring a person to provide information, like internet records, text messages, or any other records, that would assist in their investigation;
- apply on a victim's behalf for a Cyberbullying Prevention Order; and
- send letters to the person engaging in cyberbullying warning them that their actions constitute cyberbullying under the *CSA*.

Through amendments to the *Education Act*, the *CSA* also enabled school boards to cooperate with the Government of Nova Scotia and its agencies, including CyberScan, to promote and encourage safe and respectful cyber communications. It also formalized the authority of school principals to respond to incidents of bullying and cyberbullying that occurred off school grounds and/or outside of school hours. The authority granted to CyberScan staff, school boards, and principals through the *CSA* remained in place until 2015.

In 2015, a challenge was brought to the Supreme Court of Nova Scotia against the *CSA* in the case of *Crouch v. Snell* ("*Snell*"). In *Snell*, it was argued that the *CSA*'s broad definition of cyberbullying and the grounds and processes for an applicant to receive a Cyberbullying Prevention Order violated Canadian freedom of expression as guaranteed by section 2(b) of the *Charter of Rights and Freedoms* ("*Charter*").

In its ruling for *Snell*, the Supreme Court of Nova Scotia found that the *CSA* was arbitrary, overbroad, vague, and procedurally unfair. That led the Court to strike down the *CSA* in its entirety. New legislation was therefore required to continue to address cyberbullying and the non-consensual sharing of intimate images, while avoiding these *Charter* shortfalls.

2.2. Intimate Images and Cyber-protection Act

In July 2018, the *Intimate Images and Cyber-protection Act* ("*IICPA*") replaced the former *Cyber-safety Act* ("*CSA*"). The *IICPA* was created to protect victims of cyberbullying and non-consensual sharing of intimate images, while avoiding the *Charter* issues that the *CSA* had faced. Under this legislation, Nova Scotians can access supports and pursue alternatives to criminal prosecution. While the *CSA* primarily addressed cyberbullying, the *IICPA* made Nova Scotia unique in its approach to address both the non-consensual sharing of intimate images and cyberbullying in the same legislation (Dodge, 2021).

The goals of the *IICPA* are to discourage, prevent, and respond to the harms of non-consensual sharing of intimate images and cyberbullying. In doing so, the *IICPA* must uphold and protect the fundamental freedoms of thought, belief, opinion, and expression, including freedom of the press and communication media.

Under the *IICPA*, several factors must be met for a communication to qualify as cyberbullying:

- the communication is carried out electronically– by email, text message, or online, such as, through social media; and
- the communication causes or is likely to cause harm to another person's health or well-being; and
- the person responsible for the communication maliciously intended to cause harm to another individual's health or well-being or the person responsible for the communication was reckless, that is, didn't think about or care if the communication might cause harm to another person's health or well-being.

For a communication to qualify as cyberbullying, it can either be directed to the person being harmed or it may be about that person.

Under the *IICPA*, the following factors must be met for an image to qualify as an intimate image:

- it is a visual recording of a person such as a photograph, film, video, or any other kind of visual recording; and
- the person in the image had a reasonable expectation of privacy when the image was recorded; and
- the person in the image is either nude, exposing their genitals or anal region, exposing her breasts, or engaged in explicit sexual activity; and
- when the image was first shared, the person in the image had a reasonable expectation of privacy, that is, they expected the image to be shared only among people of their choosing.

To share an intimate image without consent means to make the image available to anyone other than the person in the image under one of two conditions:

- the person sharing the image knew that the person in the image did not consent to its distribution; or
- the person sharing the image was reckless, that is, didn't care to find out if the person in the image had consented to its distribution, including publishing, advertising, selling, transmitting, or distributing the image in any way.

The *IICPA* and its regulations allow victims of cyberbullying or non-consensual intimate image distribution, or parents if the victim is a youth, to initiate a voluntary court process for private legal disputes. This process can lead the Supreme Court of Nova Scotia to grant a statutory Cyber-protection Order.

A Cyber-protection Order is distinct from the Cyberbullying Prevention Order that had been available under the *CSA*. While there were no criteria set out under the *CSA* for the Court to consider when ruling whether to grant a Cyberbullying Prevention Order, section 6(7) of the *IICPA* lays out 13 factors that the Court should weigh when ruling whether to grant a Cyber-protection Order:

- the content of the intimate image or cyberbullying;
- the manner and repetition of the conduct;
- the nature and extent of the harm caused;
- the age and vulnerability of the person depicted in the intimate image distributed without consent or victim of cyberbullying;
- the purpose or intention of the person responsible for the distribution of the intimate image without consent or the cyberbullying;
- the occasion, context, and subject-matter of the conduct;
- the extent of the distribution of the intimate image or cyberbullying;
- the truth or falsity of the communication;
- the conduct of the person responsible for the distribution of the intimate image or cyberbullying, including any effort to minimize harm;
- the age and maturity of the person responsible for distribution of the intimate image without consent or cyberbullying;
- the technical and operational practicalities and costs of carrying out the order;
- the *Canadian Charter of Rights and Freedoms*; and
- any other relevant factor or circumstance.

If the Supreme Court of Nova Scotia reviews an application and decides that there are grounds to issue a Cyber-protection Order, they can:

- forbid someone from sharing an intimate image;
- forbid someone from posting communications that would be considered cyberbullying;
- forbid someone from contacting the victim in the future;
- order a person to take down or disable access to an intimate image or communication;
- declare that an image is an intimate image or that communication is cyberbullying;
- refer the parties to dispute resolution; and
- award damages to the victim.

If an individual does not know the identity of the cyberbully or individual/entity who shared their intimate image, they can also apply for an order from the Court that would require either an individual or company (such as a social media company or an internet service provider) to help identify the individual or entity.

2.3. Implementation of the Intimate Images and Cyber-protection Act

The process of addressing cyberbullying and the non-consensual distribution of intimate images changed considerably under the *Intimate Images and Cyber-Protection Act* ("*IICPA*") compared to that of the *CSA*. The *IICPA*'s definition of cyberbullying was considerably narrowed to ensure that it did not include instances of legitimate free speech and aligned with the *Charter*. Significant changes to the definition of cyberbullying include that the conduct must be malicious or reckless, and either cause, or be likely to cause, harm to another individual's health or well-being.

The *IICPA* allows the Minister of Justice to designate an agency to:

- provide public information and education regarding harmful on-line conduct;
- advise public bodies on policies for online safety and conduct;
- provide support and assistance to victims of intimate image distribution without consent and cyberbullying;
- provide information to victims of intimate image distribution without consent and cyberbullying respecting the criminal justice system and proceedings under this Act;
- provide information to victims of intimate image distribution without consent and cyberbullying respecting contacting police;
- provide voluntary dispute-resolution services, including advice, negotiation, mediation, and restorative justice approaches in respect of harmful on-line conduct; and
- provide such other services, exercise such other powers and authorities and perform such other duties as may be prescribed by the regulations.

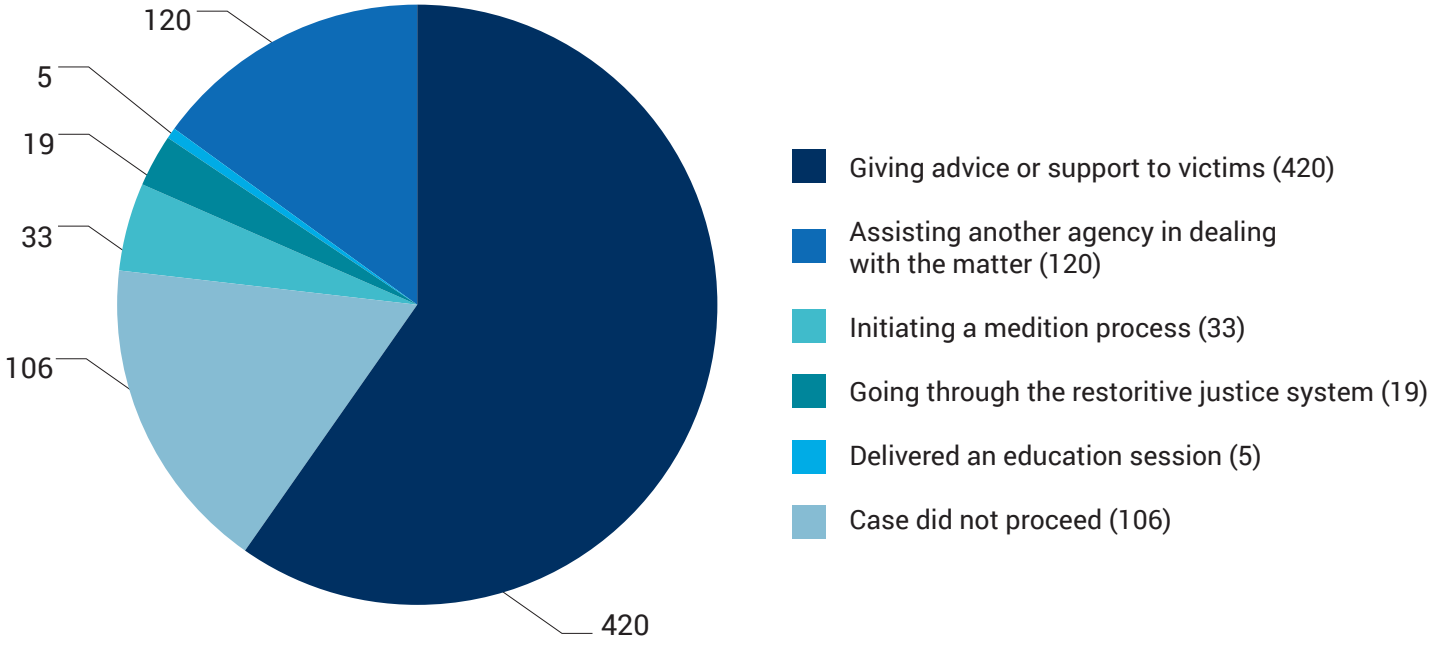
Under the *IICPA*, the CyberScan unit at the Department of Justice focuses on informal victim supports, including those mentioned above. They can support victims in submitting take-down requests to digital platforms for images or posts to be removed and explore dispute resolution possibilities. CyberScan staff also collaborate with stakeholders such as teachers, school administrations, and community organizations across Nova Scotia to provide education and information about cyberbullying and non-consensual intimate image distribution.

Between July 2018 and March 2022, CyberScan staff opened 703 cases in Nova Scotia. CyberScan keeps records of safety concerns that individuals report to identify trends and improve its services. The most frequently cited safety concerns from victims were:

- nasty comments or name calling;
- threats, intimidation, or menacing comments;
- false allegations;
- fake or impersonated accounts;
- unwanted contact or harassment;
- the non-consensual distribution of a youth's intimate images;
- the non-consensual distribution of an adult's intimate images; and
- inciting or encouraging an individual to self-harm or commit suicide.

CyberScan staff record cases by type of support to further identify trends in cyberbullying and non-consensual intimate image sharing, see following graphic.

Nature of CyberScan Cases from July 2018 to March 2022



In addition to these responses, CyberScan staff have offered over 500 presentations reaching over 16,000 youth and adults. These presentations were offered in school and community settings with a focus on themes of cyber safety and the mandate of the CyberScan unit.

Under the *IICPA*, CyberScan staff can no longer apply for a court order on a victim's behalf. Victims can pursue private legal action through a statutory Cyber-protection Order under the *IICPA* (See: 2.2. *Intimate Images and Cyber-protection Act*). If that action is taken, it becomes the responsibility of the Court to determine whether a Cyber-protection Order is warranted.

The first case brought to the Supreme Court of Nova Scotia that involved *IICPA*'s statutory tort for cyberbullying was *Candelora v Feser* ("*Candelora*"), 2020 NSSC 177. In *Candelora*, the Court awarded damages of $85,000 to a victim of cyberbullying, who had been subjected to "a campaign [that] took the form of a long series of venomous Facebook postings" (Harris, 2020). *Candelora* highlighted that once the Court is satisfied a person has engaged in cyberbullying under its *IICPA* definition, it will rule in favor of the applicant and then look to the specific facts of the case to determine what type of order is warranted and whether damages should be awarded (Harris, 2020). It is possible that the awarded damages in *Candelora* may deter future cyberbullying and non-consensual sharing of intimate images.

While *Candelora* demonstrated that the *IICPA* can be used for victims to get recourse, it has been suggested that the *IICPA* creates barriers to access to justice for victims because they must go through the Nova Scotia Supreme Court, which is a process that is resource intensive, lengthy, and can be confusing for self-represented parties (Fraser, 2017).

The *IICPA* has been in effect since July 2018 and this review allows for consideration of the effectiveness of both the *Act* and its implementation.

Research

3.1. International Perspectives

When considering Nova Scotia's response to cyberbullying and non-consensual intimate image distribution, it is valuable to look at work being done by other countries.

Australia has an independent statutory office called eSafety which operates across the country. eSafety aims to protect both adults and minors across most online platforms and forums where people can experience harm (eSafety Commissioner, 2021). It sets clear expectations for online service providers that makes them accountable for the safety of people who use their services and has created requirements for digital platforms to regulate illegal and restricted content (eSafety Commissioner, 2021). Unlike Canada, Australia has no federal legislation that prohibits the non-consensual distribution of intimate images, but several Australian states have enacted various laws which deal with related elements (Department of Justice, 2013).

While cyberbullying is not criminalized by any specific law in the United Kingdom (U.K.), it is similar to Canada in that by committing an act of cyberbullying, a person may be committing a criminal offence under other acts (See: 4.2.1. *Criminal Code of Canada*). The U.K. shares another similarity to Canada, in that it has a federal law that prohibits the non-consensual distribution of intimate images. Under section 33 of the *Criminal Justice and Courts Act 2015*, the U.K. criminalized 'revenge porn,' which is a broad term for scenarios involving non-consensually uploading intimate sexual images of an individual onto the internet and made it punishable by up to a maximum sentence of 2 years' imprisonment (Crown Prosecution Services, 2017). In Canada, a person can be guilty of distributing another person's intimate images if that person had a reasonable expectation to privacy. In the U.K., a person is only guilty of the offence if they intended to cause distress by disclosing the intimate image to others (Crown Prosecution Services, 2017).

In the United States, there are no federal laws that specifically apply to cyberbullying, but many states have taken action to address it (Department of Justice, 2013). Most state laws, policies, and regulations require school districts to explicitly define bullying and cyberbullying, implement anti-bullying policies, and create procedures for investigating and responding to cyberbullying when it occurs (Department of Justice, 2013). Like some of the *Charter* issues faced by Nova Scotia's original *CSA*, many states have had difficulty reconciling the prevention of cyberbullying with the guaranteed rights given to Americans through the *First Amendment of the United States Constitution*.

3.2. Canadian Jurisdictional Scan

Non-consensual sharing of intimate images

Like Nova Scotia (See: 2.2. *Intimate Images and Cyber-protection Act*), the provinces of Alberta, Saskatchewan, Manitoba, New Brunswick, Newfoundland and Labrador, and Prince Edward Island have all created torts to address the non-consensual distribution of intimate images. These torts effectively establish civil liability for what is already a criminal offence under section 162.1 of the *Criminal Code of Canada* and can be used to provide injunctive relief or entitle victims to compensation for damages suffered.

In comparison with Nova Scotia's legislation, each provincial legislation has some similarities and differences. Like Nova Scotia, Alberta's tort authorizes the Court to make an order prohibiting the publication of the name of a party to the action. New Brunswick's tort imposes an automatic publication ban when cases are brought forward. It also allows for the victim to make their intimate image inaccessible to other people.

Compensation for the non-consensual distribution of intimate images in Saskatchewan and Alberta can be awarded without proof of damages. In Saskatchewan and Newfoundland and Labrador, there is a reverse onus on the defendant, which means that they must prove that they had consent from the person depicted to distribute their intimate images.

British Columbia has begun a consultation process on these issues and, in the future, may enact its own tort for the non-consensual distribution of intimate images. Nunavut, the Northwest Territories, and Yukon do not currently have torts to address the non-consensual distribution of intimate images.

Cyberbullying

Torts related to cyberbullying in Canada are less common. However, the Ontario Superior Court of Justice created the tort of internet harassment in 2021 for the case *Caplan v Atas*, 2021 ONSC 670 ("*Caplan*"). During their remarks, Justice Corbett noted that Nova Scotia's *IICPA* would be applicable to *Caplan*, and that the requirements of the new tort of internet harassment was a means to distinguish between conduct that is merely annoying from serious and persistent harassment that requires legal intervention (Rubin & Taylor, 2021).

Criminal Code of Canada

In March 2015, Canada amended the *Criminal Code of Canada* ("*Criminal Code*") to include the offence of publication and distribution of intimate images without consent (R.S.C., 1985, c C-46, s.162.1). Punishments available for those found guilty of this offence include a prison term of up to five years, and prohibition orders preventing the offender from using the internet or restricting their usage. There are also additional amendments that facilitate the removal of such images from the Internet, the recovery of expenses incurred to obtain the removal of such images, and the forfeiture of property used in the commission of the offence.

While certain acts of cyberbullying or non-consensual intimate image distribution may violate sections of the *Criminal Code*, they are not considered criminal matters under the *IICPA* (Department of Justice, 2017). Across Canada, the total number of people charged in connection to those acts is very low compared to the number of cases opened. Most of the cases that were taken to police either lacked evidence, were dealt with outside of a criminal court, were proven to be unfounded, or saw the victim ultimately choose to not proceed with the case (Allen, 2019).

There are currently no specific provisions in the *Criminal Code* for bullying or cyberbullying. However, depending on the nature of the activity involved, various *Criminal Code* offences may apply to instances of cyberbullying, including:

- criminal harassment (section 264);
- uttering threats (section 264.1);
- intimidation (subsection 423(1));
- mischief in relation to data (subsection 430(1.1));
- unauthorized use of computer (section 342.1);
- identity fraud (section 403);
- extortion (section 346);
- false messages, indecent or harassing telephone calls (section 372);
- counselling suicide (section 241);
- defamatory libel (sections 298-301);
- incitement of hatred (section 319); and
- child pornography offences (section 163.1).

This means that local police agencies can be contacted if incidents involve:

- making any threats of physical harm or violence;
- sending and sharing sexually explicit or intimate photos of someone under the age of 18;
- stalking a victim: where a bully is persistently following or communicating with someone in a harassing way that has them fearing for their safety; or
- using someone else's identity or accounts to facilitate the bullying or harassment.

3.3. Environmental Scan

Due to the COVID-19 pandemic, many Canadians have experienced extended periods of isolation from friends and peers and an increase in daily screen time. A study of 254 Canadian families reported increased screen times in mothers, fathers, and children during the pandemic at 74%, 61%, and 87%, respectively (Caroll et al., 2020).

Children and youth

This was especially impactful for children and youth as they transitioned to remote learning. Researchers from Western University found that during the COVID-19 pandemic, Canadian youth have had an average of six hours of screen time each day, with some having as much as 13 hours (Seguin et al., 2021). That greatly exceeds the recommended two hours a day for youth. Since youth have often been prevented from seeing their friends and peers over the past two years, many have increased their social media usage. Social media is known to amplify cyberbullying, so when a youth's social media usage goes up, so does their risk of being cyberbullied (Suciu, 2021).

Researchers in Ontario found that among a sample of just over 2,000 Ontario youth, a correlation existed between increased screen time, and mental health and behavior problems (Li et al., 2021). The impact of that correlation was noticeable across Canada by the fall of 2020, when it was reported that since the start of the pandemic, Kids Help Phone had experienced an increase in demand for its services from Canadian youth (Buckner, 2020). In 2020, it was estimated that 4 million young Canadians reached out to Kids Help Phone (Yousif, 2020).

Social norms

Cyberbullying has become normalized on many social media platforms. Companies that run social media platforms often cannot track cyberbullying occurrences because their chat features use end-to-end encryption, for example WhatsApp and Snapchat. On public social media platforms like Facebook or Instagram, cyberbullying is known to be a common occurrence.

The sharing of intimate images or 'sexting' has become a normalized part of culture as well (Government of Canada, 2021). Sexting can be a difficult issue to navigate, because although exploring sexuality is a normal and healthy part of life, it quickly becomes illegal when non-consensual sharing of intimate images occurs (Government of Canada, 2021). Youth may have an incorrect belief that most of their peers are sexting, which may make them more likely to share intimate images, even if they are not comfortable doing so (eSafety Commissioner, 2017).

It is known that Canada has seen a significant increase in non-consensual intimate image sharing since the beginning of the COVID-19 pandemic. Looking at data from Statistics Canada (2021) for the first seven months of the pandemic, it seems that Canada was on track to see an 80% increase in reported incidents of non-consensual intimate image distribution compared to the five-year national average.

Removal requests

Many social media sites have established content policies and feature accessible channels to report content that is abusive or involves non-consensual intimate images and request that it be taken down. In 2017, the Supreme Court of Canada ruled that Canadian common law courts have the jurisdiction to make orders against search engines like Google, Bing, and Yahoo (Sookman, 2017). This means that Canadian common law courts, such as the Supreme Court of Nova Scotia, can order search engines to take down URL links of images that have been shared without consent. In addition, several search engines like Google and Bing allow for victims to directly request the removal of URL links.

It is also possible to report cyberbullying and the non-consensual distribution of intimate images to internet and mobile service providers. Most of these providers have 'acceptable use' policies in place, so if there is evidence to prove that a user has violated those terms, providers may issue a warning or even suspend or terminate a user's account when warnings are ignored.

If a victim initiates a civil action under the *IICPA*, the Court can also order the guilty party to take down the digital content as part of a Cyber-protection Order (See: 2.2. *Intimate Images and Cyber-protection Act* and 2.3. *Implementation of IIPCA*).

Education settings

School communities have a key role in addressing cyberbullying and the non-consensual distribution of intimate images. School staff can connect children and youth with support services, including CyberScan. Principals and school administration have the authority to address all incidents of bullying when such behaviour significantly disrupts the learning climate of the school, whether in-person or electronic, onsite or outside of school property. Dr. Alexa Dodge notes that schools, government, community agencies, police services, students, and families need collaborative pathways to respond to cyberbullying and the non-consensual sharing of intimate images (2021).

There is an opportunity to further deter cyberbullying and non-consensual sharing of intimate image sharing in education settings. The current cyber safety model of education in Nova Scotia primarily places responsibility on potential victims to protect their online privacy and to avoid online interactions with strangers. This may contribute to a normalization of the actions of perpetrators who make the decision to cyberbully and/or share intimate images without consent (Dodge, 2021).

CyberScan continues to be an informal support for children and youth experiencing cyberbullying and the non-consensual distribution of intimate images. When students share these experiences with school staff, they are often connected with CyberScan staff. As noted by Dr. Dodge (2021), there is an opportunity for CyberScan staff to document specific types of discrimination that victims have experienced in connection with these issues, as doing so could help highlight patterns and support the creation of targeted educational and awareness campaigns.

Dr. Dodge has suggested that best practices in addressing cyberbullying and non-consensual intimate image distribution in education settings should focus on teaching the importance of healthy and ethical relationships, consent, and empathy (2021).

Public Consultation

4.1. Overview

Evoke Consulting was hired to design a public consultation process and deliver interactive sessions with stakeholders across the province. The consultation took a trauma-informed approach to discussing the sensitive topics of non-consensual intimate image sharing and cyberbullying. The process was inclusive by design and prioritized the participation of diverse stakeholders and those with direct experiences related to the *IICPA*.

The objectives of the consultation were to:

- deepen the understanding of the public/stakeholders' lived experiences related to the *IICPA* and its delivery;
- uncover stakeholder observations, challenges, and needs; and
- identify opportunities.

Interdepartmental Working Group

An Interdepartmental Working Group ("Working Group") was formed with staff from within divisions and departments to inform the review of the legislation and the development and delivery of the public consultation.

The Working Group facilitated a full spectrum of connections to stakeholders across Nova Scotia for engagement and the ability to create spaces for meaningful feedback on the *IICPA*. They provided input for stakeholder engagement methods when working with youth and marginalized community members as well as insights on approaches that respected the voices of vulnerable Nova Scotians, such as victims of non-consensual intimate image sharing and/or cyberbullying, while maintaining safety, confidentiality, and anonymity. The Working Group made sure that the consultation connected with stakeholders in urban and rural areas across Nova Scotia and promoted participation in the public consultation and engagement processes within government and with external stakeholders.

The Working Group included staff from such departments as the Department of Education and Early Childhood Development, the Department of Municipal Affairs and Housing, and the Department of Justice. Membership was made up of staff specializing in areas such as Victim Services, Cyberbullying, Diversity and Inclusion, and Restorative Approaches.

4.2. Methods

The consultants took a three-pronged, human-centred approach to uncovering insights on how the *IICPA* is achieving its purpose. First, they reviewed existing Department of Justice materials and research and learned from staff experiences. Second, they heard directly from Nova Scotians by facilitating 19 interactive consultation sessions. Finally, they provided the public with a channel to voice their perspectives through an online survey.

Once sessions were complete, the consultants completed sensemaking of the data collected. This stage included pattern and thematic analysis of virtual sessions and quantitative and qualitative survey results. Finally, a 'What We Heard' report was completed and presented to the Working Group and Department of Justice staff, including findings, insights, and opportunities.

Consultation research questions

The following research questions were developed to uncover specific insights from those directly and/or indirectly impacted by the *IICPA*:

1. What is your personal experience with cyberbullying, and/or intimate image sharing without consent? If comfortable, please tell us about your experience.
2. Do you think this law helps to discourage and prevent cyberbullying and intimate image sharing without consent? Why or why not?
3. Do you think this law upholds and protects the fundamental freedoms of thought, belief, opinion, and expression, including freedom of the press and other media of communication? Why or why not?
4. Do you think this law helps Nova Scotians respond to non-consensual sharing of intimate images and cyberbullying? Why or why not?
5. Overall, do you think this law is effective? Why or why not? What works well? What is most challenging or the greatest area of opportunity? What suggestions do you have for how the Government of Nova Scotia can best support people who have a personal relationship to non-consensual intimate image sharing and/or cyberbullying?

These questions were used to guide discussions in small group sessions and individual conversations and were adapted for inclusion in the public survey. Questions were not used as a script, rather as guideposts to start conversation and provide insight and discovery.

While questions were standardized to ensure consistency in response and data outputs, adaptability was prioritized to be inclusive of stakeholder experiences. This allowed for flexibility when participants communicated or showed discomfort with scripted questions. In these instances, facilitators were able to pivot and create the space for conversation, asking related questions and dialogue while staying true to research and trauma-informed principles.

Consultation planning considerations

In accordance with public health guidelines related to the COVID-19 pandemic, it was determined that planned in-person consultation sessions would be adapted to take place virtually to ensure the safety of all stakeholders. This shift to virtual participation allowed a greater number of sessions to take place.

Stakeholders were provided flexible options to participate in terms of timing and engagement methods, including supports for participants with disabilities. Providing choice to victims on how to share their experiences and available supports ensured that the process was inclusive and respectful. Due to the sensitive nature of the topics covered, participants were reminded that the process of sharing their experience was voluntary and confidential and that participants could opt out of the engagement process at any time.

In alignment with best practice in stakeholder engagement, two consultants were present for each interactive session. One consultant led and facilitated the session while the other observed and engaged with less active participants thereby creating a safe environment for sharing and connection to appropriate supports. This approach was particularly important in this consultation due to the topics of personal relationships, intimate images, and the impacts of cyberbullying.

Sessions were not recorded using video or audio, a standard in human-centered sessions, particularly given the subject matter. This was stated both in participant invitations and at the start of each session, along with other key messages, including the commitment to protecting privacy and anonymity.

Dr. Dayna Lee-Baggley was a named resource on the consultation team. As a registered clinical psychologist, she acted as a subject matter expert in trauma-informed practices and prioritized the safety and wellness of participants. Victims were invited to include one or two support persons in conversations if they felt that would be helpful. They were also provided access to Dr. Lee-Baggley to debrief the experience of telling their story and learn about connections to mental health resources.

Inclusive by design

At the beginning of the consultation design process, it was determined that a consultation tool would be developed to ensure inclusion of diverse perspectives.

A selection tool was created to support inclusive participant selection processes. This tool was designed to make certain the consultation was inclusive of lived experiences related to the *Act* and reflective of the diversity in Nova Scotia and those who interact with the *Act*. The following steps were taken to facilitate access and participation in the process:

- alternative options for engagement were created so participants could share their experiences in ways that were comfortable and accessible;
- interactive sessions were complimented with an online survey to share with informal networks;
- Government of Nova Scotia promoted participation in the consultation and engagement process through website, social media platforms, including Facebook and Twitter;
- communications were created using plain language and the website and online survey were available in English and French; and
- Department of Justice contact email and phone information was shared in communications for participants who needed support to access or complete the survey.

Participant selection

The Working Group recognized that marginalized communities may be disproportionately impacted by the *Act* and worked collaboratively to support an equitable participant selection and engagement process. Organizations and networks were identified to support an inclusive design and delivery process.

The importance of recognizing the many aspects of human diversity in Nova Scotia was discussed in the Working Group to ensure that the participant selection process was inclusive. Some of the aspects of human diversity discussed included, but were not limited to; age, geography (i.e. location in Nova Scotia), identification with community, gender identity, cultural background, socioeconomic background, ability, language, and other forms of human difference.

A participant selection tool was developed, using scales to prioritize interactive participation with those directly impacted by the *Act* and with diverse perspectives, see Appendix A. Interactive participation included small group sessions and individual conversations.

Small group discussions

There were eleven small group sessions conducted with public and professional stakeholders. Sessions were held using online platforms such as Zoom and Microsoft Teams and varied in length from 60-90 minutes. Each session included a maximum of 6 participants to ensure that all voices and perspectives were heard.

There were 59 participants in the small group sessions offered in collaboration with stakeholders across Nova Scotia representing rural, suburban, and urban communities.

These group sessions were inclusive of the diversity of Nova Scotian experiences with participants who identified as Indigenous, African Nova Scotian, and Acadian/ francophone community members. Sessions were designed and delivered to engage with specific groups of individuals and professionals such as law enforcement, youth, persons with disabilities, and education stakeholders.

One-to-one conversations

The consultation included eight, one-to-one conversations; five with victims of non-consensual intimate image sharing and/or cyberbullying and three with legal and academic professionals. Conversations varied in length from 30-60 minutes.

Online survey

An online survey was developed to encourage broad public participation in the consultation and encourage feedback from the public who may or may not have had direct interaction with the *IICPA* and the issues of non-consensual intimate image sharing and/or cyberbullying.

The online survey was offered via Select Survey in English and French and was open for public participation from January 6- 28, 2022. The Working Group helped to raise awareness and increase participation in the online survey through internal and external networks.

The survey allowed for an unlimited number of responses and included opportunities for the public to share their experiences in connection with the *IICPA* and related issues. There were 399 individuals who completed the survey, including 184 open-ended/qualitative responses.

It was important to learn what personal experience survey respondents had with the *Act*, while recognizing that experiences may be complex. The survey was designed with this in mind, allowing respondents to self-identify with more than one personal experience.

Survey results

Analysis was completed on both quantitative and qualitative responses from the 399 unique survey respondents. The following is a summary of the results:

Question	Responses
What is your personal experience with cyberbullying and/or intimate image sharing without consent? Please select all categories that apply to you.	34% Professional 30% No direct experience 22% Victims 13% Family members/friends/partners 8% Parents/guardians 6% Prefer not to say 4% Other Note: The above responses total more than 100% due to respondents' ability to select more than one personal experience category.
Use the scale provided to tell us how much you agree/disagree with the following statements. (1 strongly disagree; 2 disagree; 3 unsure; 4 agree; 5 strongly agree) *This law helps to discourage and prevent cyberbullying and intimate image sharing without consent.*	46% of survey respondents selected strongly agree or agree. 28% of survey respondents selected strongly disagree or disagree.

Use the scale provided to tell us how much you agree/disagree with the following statements. (1 strongly disagree; 2 disagree; 3 unsure; 4 agree; 5 strongly agree) *This law upholds and protects the fundamental freedoms of thought, belief, opinion, and expression, including freedom of the press and other media of communication.*	54% of survey respondents selected strongly agree or agree. 13% of survey respondents selected strongly disagree or disagree.
Use the scale provided to tell us how much you agree/disagree with the following statements. (1 strongly disagree; 2 disagree; 3 unsure; 4 agree; 5 strongly agree) *This law helps Nova Scotians respond to non-consensual sharing of intimate images and cyberbullying.*	55% of survey respondents selected strongly agree or agree. 21% of survey respondents selected strongly disagree or disagree.
What suggestions do you have for how the Nova Scotia Government can best support people who have a personal relationship to non-consensual intimate image sharing and/or cyberbullying? (optional, open-text)	46% of survey respondents shared suggestions, with the following key themes: • need for coordinated victim supports • need for public awareness and education in connection with the *IICPA* • barriers to initiating action, including financial barriers • need for training/inclusive language in connection with the *Act* • need for timely responses to those experiencing non-consensual intimate image sharing and cyberbullying to reduce risk of harm

4.3 Findings

Most participants in the consultation shared that the *Act* strikes a good balance between protecting their freedoms and protecting citizens from cyberbullying and non-consensual sharing of intimate images. This section summarizes insights and opportunities from the online survey, small group sessions, and one-to-one conversations to improve upon the *Act* and its delivery.

Changes associated with who and how people interact online are impacting instances of non-consensual intimate image sharing and cyberbullying.

Participants shared that, at all ages, the sharing of intimate images without consent and cyberbullying are becoming increasingly normalized. As a result, participants felt it can be challenging to affect behaviour change in relation to normalized attitudes. Participants from all backgrounds described witnessing and/or experiencing social and peer pressure from friends or partners to share intimate images. Although these issues impact all Nova Scotians, some community members may be more vulnerable than others, including youth, people with intellectual disabilities, people with low technological literacy, and seniors.

Technology usage among children and youth emerged as a theme throughout the consultation. Participants shared that most children/youth they interact with have mobile devices with data and access to the internet and apps. Parents/guardians/teachers shared that it is challenging for them to keep up with social media trends. They shared that they could benefit from improved knowledge of technology and increased awareness of online behaviour of children and youth.

There are multiple barriers related to accessing, understanding, and using the *Act*.

Awareness of the *Act* was lacking across all stakeholder groups who participated in the consultation. Most participants, ranging from law enforcement to victims and the public, were unaware of the *Act* and associated civil processes. Participants shared multiple barriers to accessing the *Act*, including but not limited to:

- lack of awareness of the *Act*;
- lack of clarity regarding civil and criminal processes;
- lack of clarity on available resources/supports;
- language that was not inclusive;
- requirement to tell stories and share personal details multiple times;
- financial barriers and cost of legal processes;
- feelings of shame, embarrassment, and helplessness;
- feelings of not being believed;

- fear of personal repercussions; and
- limited access points to CyberScan services.

Most victims reported experiencing confusion when seeking support. They said they felt helpless in their efforts to be taken seriously and described a lack of clear choices for action. Victims described additional barriers to seeking support such as feelings of shame, a fear of consequences like job loss, concerns about reputation, and fear of increased violence.

Participants reported a need for CyberScan staff to use inclusive language in connection with the *Act* around gender-identity and diverse experiences as well as a need for additional access points to CyberScan. Financial barriers to proceeding with civil action were highlighted by participants across stakeholder groups.

Stakeholders shared that efforts to educate about these issues are already in development or underway in some communities. The consultation highlighted a need to educate all Nova Scotians about the *Act* and related supports, including parents, vulnerable populations, law enforcement, and community-based organizations.

"It is now 2022, the only way to report online abuses is through a phone call? The CyberScan website only lists 2 phone numbers to contact. No email, no SMS, no real-time chat. Not even an online form to fill out. No options for people using TTY devices or other assistive devices." (Family member/friend/partner)

Acceptable and unacceptable behaviour can be better defined with consideration for desired outcomes of those impacted.

Stakeholders shared a strong need for awareness campaigns related to the *Act* and potential consequences. There was an identified need for diverse approaches to campaign design and delivery to reach target audiences, including vulnerable populations.

Adult participants shared that the term 'cyberbullying' doesn't resonate with them, and promotional materials could be designed to better reflect adults in connection with the *Act*. Public awareness campaigns may have focused on youth in the past, however this issue impacts adults and youth, particularly within intimate partner relationships. Some adult participants were unaware of the consequences of sharing intimate images without consent.

These issues are complex, and stakeholders shared the need for plain and accessible language to better define CyberScan services and action steps. This supports the trauma-informed approach mentioned by consultation participants to support victims in making informed decisions.

Victims shared the challenge of navigating multiple barriers in their lives in addition to experiences of cyberbullying and/or non-consensual sharing of intimate images. Civil or criminal processes may not be a victim's principal focus. Whether stated directly by victims or described by others (legal expert, law enforcement, educator), the most desired outcome shared was to 'make it stop.'

"The information has to be shared more widely as a lot of people are not sure of the law and exactly how it pertains to them." (Professional)

Navigating complex government systems can result in increased risk to victims.

The complexity of the system is a barrier to desired outcomes and stakeholders shared that victims are at risk of falling through the cracks.

Some components of the *Act* can be related to the *Criminal Code* such as distribution of intimate images, harassment, and uttering threats. These require evidence that proves a crime has been committed. Multiple government departments, courts, and organizations may be involved in a single case due to complex circumstances. Victims who are experiencing unsafe situations related to intimate image sharing and cyberbullying may be put at greater risk when navigating complex government systems.

Victims shared that they could benefit from a collaborative support system equipped to navigate the complexity of their situation with guidance and pathways for support whether related to civil or criminal activity. Participants shared the need for multiple entry points to the CyberScan intake process.

The requirements placed on victims significantly impact their decision to proceed, persist, and seek support.

"What would have made the experience better? If the threats were taken seriously. If they could hold her responsible, investigate if it is her. I was responsible to collect everything. I have a drive with everything saved - a file folder saved with dates, times, screenshots on everything she's done; she has typed admitting to doing this… what more is needed?" (Victim)

Victims described systemic requirements that were challenging to navigate, such as retelling their experiences to multiple stakeholders, verifying elements of their claim, and record-keeping. They described the need for a consistent support person/advocate to navigate supports during their experiences of non-consensual intimate image sharing and/or cyberbullying. Processes for victims, from beginning to end, require resources and abilities that may present barriers for many Nova Scotians such as high levels of technical literacy and language competency. These processes also require internet access, printer access, and significant financial resources for legal support.

Stakeholders shared a need for targeted supports for victims of cyberbullying and non-consensual sharing of intimate images such as counselling and legal advice. Those victims who had the support of a partner or employer shared that they couldn't imagine going through it alone. Some victims shared that they paid for legal representation and counselling to navigate the impacts of their experiences and the civil process.

The public consultation was successful in providing a broad understanding of Nova Scotians' lived experiences related to the *Act* as well as insights and opportunities. The following sections explore these insights in depth and outline recommendations for the *IICPA* to continue to achieve its goals.

Advancement of Technology and Social Norms

5.1. Introduction

Technology is advancing at unprecedented rates. This reality, coupled with an increase in online interaction has created an environment where the risk of cyberbullying and/or non-consensual sharing of intimate images has increased as well. The *IICPA* plays an important role in keeping the public safe in such interactions. Educators, administrators, youth, and members of the community are witnessing or experiencing social pressures to participate in actions falling under the *Act*.

The stakes are high for youth: many children, aged as low as eight years old, have access to the internet and are interacting with few safety mechanisms in place. Some Nova Scotians may be at elevated risk due to vulnerability, including individuals who may not comprehend the consequences of their online interactions.

Rapid changes in technology also create barriers to identifying issues and implementing solutions. Community leaders are finding it challenging to keep pace with social media trends and platforms and many parents/guardians and teachers are not equipped to help youth recognize the difference between safe and unsafe decisions online. Educating Nova Scotians on how and when to seek support when facing issues related to cyberbullying and/or non-consensual sharing of intimate images has become critical.

5.2. Opportunities to respond to new technologies and norms

Affecting normalized behaviour and attitudes is a daunting but necessary task to encourage the public to seek support for incidents of cyberbullying and/or non-consensual sharing of intimate images. Given the rise of these incidents, we must consider how to encourage incident reporting.

Creating accessible education and awareness campaigns will be essential to an increase in incident reporting. Demonstrating how cyberbullying and/or non-consensual sharing of intimate images impacts the community at large will help to reduce stigma and alienation. When possible, sharing real life experiences of community members may help break down barriers to seeking support. It is equally important for campaigns to be empowering and action-oriented to encourage victims to access support services.

There is a risk of additional strain being placed on victims while navigating the reporting process, with a high degree of the burden of proof being placed on them. In some cases, a victim may be asked to relive their traumatic experience, causing the individual more harm through re-victimization. To prevent this cycle, it is essential for all victims reporting incidents to have access to trauma-informed services. Awareness, accessibility, inclusion, and collaboration are key factors for providing effective support services and creating pathways to resolution.

5.3. Recommendations

Build in methods to assess technological advancements, online trends, and opportunities for collaboration with stakeholders to enable continuous process improvements within CyberScan.

Given the pace of change and growing instances of cyberbullying and non-consensual intimate image sharing, staying up-to-date on technological advancements and online trends can pose a significant challenge. A culture of collaboration and continuous improvement will allow CyberScan staff to achieve this goal.

A two-way channel of communication between the CyberScan unit and subject matter experts can support further improvements and the knowledge of technological advancements can be shared with community partners, educators, law enforcement, and guardians to ensure that all stakeholder groups are informed.

Awareness and Accessibility

6.1. Introduction

The majority of Nova Scotians surveyed were unfamiliar with the *IICPA*. Community leaders and law enforcement also had a low level of familiarity with the *Act*.

Consultation participants also shared uncertainty about how to proceed when seeking support or reporting an incident. This lack of awareness does not pertain to the *IICPA* itself, but on how to seek support and services. In these cases, increased public awareness and consistent messaging when outlining action steps will be key to effective victim support.

6.2. Opportunities to strengthen public awareness and pathways for access

The Department of Justice has an opportunity to develop awareness campaigns using various communication channels, including advertising on social media platforms that will extend audience reach. A robust communication plan can also clarify pathways for support based on common language and understanding.

All Nova Scotians with access to technology are at risk of being a victim of cyberbullying and/or non-consensual sharing of intimate images, therefore it is important to keep support as accessible as possible. Currently, the public's only incident reporting channel is via CyberScan phone numbers, where victims must disclose a great deal of personal information. This intake channel can deter Nova Scotians from seeking support. Providing foundational resources to potential victims can clarify parameters of available supports and required information for the intake process. These resources may include guides on how to prepare and what to expect when reaching out to CyberScan as well as contact information for other relevant supports.

During the public consultation, some victims reported feelings of helplessness, noting a lack of being taken seriously when receiving government supports and services. These individuals felt the need to be persuasive in their tone and convincing simply to be heard. This may be related to the blame and fear some victims experienced from their own role in their situation. In some cases, victims shared that escalation of behaviours resulted in exposure to life-threatening situations.

Nova Scotians have many potential routes to initiating action if they are impacted by cyberbullying and/or non-consensual sharing of intimate images. However, not all routes arrive at the same outcome. Some access points are less familiar with how to handle complaints under the *IICPA*, leading to inconsistency and confusion. As it stands, there is not a clearly understood course of action for those seeking support.

Educating Nova Scotians on matters pertaining to the *IICPA* can strengthen public awareness while simultaneously improving access. Different audiences have unique needs which must be considered when creating awareness campaigns to ensure that Nova Scotians understand the *Act* and fully realize the benefits of available supports.

6.3. Recommendations

Increase knowledge of the *IICPA* and CyberScan through presentations and public awareness campaigns, including targeted delivery methods for various demographics.

Nova Scotians need clarity on the *IICPA* and how they can interact with it. The objectives of the *Act* need to be clear and consistent across all platforms, including presentations, awareness campaigns, and communications with victims. An essential point to demonstrate is how people can access resources such as CyberScan.

There is an opportunity to create familiarity with the *IICPA*, help individuals identify if they are being victimized, and outline where they can go for support. For youth, advertisements on social media apps and educating school staff present effective opportunities to expand the reach of CyberScan. For adults, social media apps like Facebook and Instagram can be used to communicate key messages in addition to government websites. Ultimately, every Nova Scotian should have basic knowledge about the *IICPA* and how to access available resources.

Clearly state potential consequences of violating the *IICPA* in awareness campaigns to discourage cyberbullying and non-consensual intimate image sharing and encourage victims to seek support.

Risk awareness is a critical preventative tool for combating cyberbullying and non-consensual intimate image sharing. Using awareness campaigns to clearly state the potential consequences of violating the *IICPA* will be an essential step toward creating an environment where the public knows and understands the risks associated with these behaviours.

At the same time, victims' increased understanding of the potential consequences of the *IICPA* can empower them to report incidents and create an environment of mutual understanding and accountability.

Clarify CyberScan access points by developing and publicizing clear parameters, including hours of operation, services offered, and communication timelines while ensuring CyberScan services are accessible.

Through the development of parameters that are made available to everyone, access to CyberScan services can be clarified. Publicizing information, including hours of operations, services available, and communication timelines, will further this goal.

The current communication pathways for initiating requests for support from CyberScan include a local phone number and a toll-free phone number. Using phone numbers as the sole pathway to request support can create barriers. Providing a variety of communication channels, including online options such as email and/or online intake forms, can help break down these barriers. A variety of communication channels will better support victims who may feel uncomfortable reporting incidents by phone and provide the option for victims to initiate requests for support outside of regular business hours.

Require CyberScan staff to complete training on trauma-informed and restorative approaches when working with victims.

It is recommended that CyberScan staff be required to complete training in trauma-informed approaches and restorative approaches. This training can prioritize the safety and wellbeing of victims as they receive support services. Victims who have experienced trauma can be triggered to reporting their experience, which can cause elevated levels of stress and anxiety. Staff who are equipped with trauma-informed practices and restorative approaches can dramatically improve a victim's experience.

Develop a centralized, trauma-informed intake process to reduce the risk of re-victimization.

Accessible entry points should funnel into a centralized intake process. CyberScan staff receive inquiries from a wide range of stakeholders including community organizations, law enforcement, education stakeholders, victims' family members, and those experiencing cyberbullying and/or non-consensual intimate image sharing. Given the broad range of inquiries, the intake process needs to provide clear explanations of available services and associated processes.

There is a risk of victims being re-victimized through the CyberScan intake process and sharing sensitive details multiple times. It is necessary to standardize the CyberScan intake process whereby victims only need to share details of their case to an assigned CyberScan staff person.

Review CyberScan service delivery through an Equity, Diversity, and Inclusion lens; monitor and integrate inclusive language to ensure program is accessible and inclusive.

To maximize effectiveness and inclusivity, CyberScan services should be reviewed through the lens of Equity, Diversity, and Inclusion. The use of non-gendered language is essential for inclusion of 2SLGBTQIA+ community members. There is an additional opportunity to explore how to best support newcomers to Nova Scotia who may be at increased risk of experiencing cyberbullying and/or non-consensual intimate image sharing. CyberScan access points can be further developed for those using a Teletypewriter (TTY), a device used to type messages through a phone line. Integrating more inclusive language and access points can improve service accessibility for all Nova Scotians.

Work with law enforcement stakeholders to build stronger referral pathways for victims who are experiencing cyberbullying and non-consensual intimate image sharing.

Collaboration with law enforcement agencies across Nova Scotia can further enhance support for victims of cyberbullying and non-consensual intimate image sharing. Ongoing partnership development between CyberScan staff and law enforcement agencies can strengthen referral pathways. In addition to police agencies, there is an opportunity to enhance collaboration with Department of Justice stakeholders, such as Corrections and Victim Services.

Creating strong, consistent communication channels can ensure that victims who may be at elevated risk of harm are supported. Facilitating access points to legal information and education can also better support victims who may require additional resources.

Continuum of Victim Supports

7.1. Introduction

Existing pathways are able to support victims as they navigate challenging situations such as non-consensual intimate image sharing and cyberbullying. However, striving for greater opportunities to support victims' needs is a critical step in the advancement of the core purpose of the *IICPA*.

Clearly defined services are essential for agencies, individuals, and victims seeking support. Ensuring awareness of proper pathways becomes critical to building a seamless process; particularly given that victims may be referred to multiple agencies and require clear information about the role of each agency and service.

Navigating complex government systems can also put unnecessary stress on the victim, increasing their risk of not getting help and/or re-victimization. Agencies working with victims and vulnerable community members must be well-informed about the *IICPA* and CyberScan services.

Complex processes can also impact whether a victim decides to proceed with a complaint and/or seek support. Currently, victims are required to validate their stories and advocate for themselves throughout the process. A high degree of consideration should be placed on the desired outcomes for those affected. Ultimately, accessibility and clarity of available supports will create the best outcomes for victims.

7.2. Opportunities to better support victims' needs

This review found a wide range of existing supports and services for victims of non-consensual intimate image sharing and cyberbullying such as CyberScan, Victim Services at the Department of Justice and police agencies, women serving organizations, youth serving organizations, schools, provincial mental health crisis lines, lawyers, and counsellors. Even with these systems of support, victims shared that they felt they were not adequately supported, and several victims shared being referred back and forth among organizations and agencies.

There is an opportunity for resolution pathways to include more coordinated support mechanisms. Collaboration across systems may better support victims' needs and help them seek resolution. It is integral to ensure that the outcomes from each individual case are aligned with the desired outcomes for those engaging with the *IICPA*. While the process itself must be simple to navigate, it remains important for victims to have options as they seek resolution based on their individual needs.

Due to varying levels of familiarity with the *IICPA*, routes for resolution can appear complex to those seeking support. Navigating through government systems can be a challenge and can cause delays across support systems. Using a case management approach and supporting victims through each step of the process may help victims to navigate these systems.

Processes related to intervention, resolution, and support significantly impact the victim's decision-making from start to finish. Initiating a course of action without a clear path ahead creates a risk that the victim may abandon their case due to fear, trauma, or other barriers. Given the courage required to report an incident of cyberbullying or non-consensual intimate image sharing, lessening the administrative burden on victims would be a positive step forward to providing better support in alignment with trauma-informed approaches.

Making the navigation process easier also advances inclusivity; currently only those with skills to navigate through the system can get the help they need. Clarity and consistency will help to ensure a simple and accommodating process for those seeking support. Accessibility is also integral to ensure that vulnerable communities have the proper tools to seek support.

7.3. Recommendations

Review CyberScan services using a victim-centered lens to determine where CyberScan fits on the continuum of victim support offered by government, community organizations, and law enforcement. Determine if, as a result of the above-noted review, a realignment of service provision is required to support the use of a victim-centered approach and connection to support services.

An in-depth review of CyberScan services, using a victim-centred lens, will identify where CyberScan belongs in the continuum of victim supports and maximize its effectiveness. Exploring cases from other jurisdictions and within other government departments and agencies can also advance this goal and create opportunities for collaboration with other existing services. A realignment can help determine if a meaningful connection is present with available resources and a victim-centered approach.

Work with Department of Education and Early Childhood Development and Regional Centres for Education to learn what support may be needed for children and youth experiencing cyberbullying and/or non-consensual sharing of intimate images, their families, and school staff.

Children and youth are particularly at risk of being victims of cyberbullying and/or non-consensual sharing of intimate images. There is an opportunity to collaborate with Department of Education and Early Childhood Development and Regional Centres for Education to learn about the issues of non-consensual intimate image sharing and cyberbullying in education settings in Nova Scotia.

Parents/guardians, families, and school staff have shared that they are facing challenges related to non-consensual intimate image sharing and cyberbullying. There is an opportunity for CyberScan staff to learn more about what is needed in education settings to respond to these issues among children and youth.

Review CyberScan services using a victim-centered lens to ensure victims are supported by caseworkers as they navigate pathways to resolution.

A comprehensive review of CyberScan services should be considered from the vantage point of victims' experiences. While other factors such as resources and capacity may shape pathways to resolution, a victim-centered lens can help to ensure that CyberScan staff can best support victims and offer them the guidance they need. For instance, how can CyberScan staff minimize complexity and advance inclusiveness throughout the process? Gaining a deep understanding of victims' experiences navigating processes will enable CyberScan staff to provide the right level of support at the right time.

Develop clear pathways for legal and mental health services for victims of cyberbullying and non-consensual intimate image sharing; include contact information for immediate crisis support in CyberScan communications.

Pathways that are clear and accessible allow victims to maximize the benefits of a full range of services, including legal and mental health services. CyberScan services can provide connections to a network of existing support structures within government, police agencies, and the community to ensure that victims are receiving appropriate support.

It is recommended that crisis supports be included in communications with victims such as email signatures, voicemail messages, and the CyberScan website. Possible crisis supports include the Provincial Mental Health and Addictions Crisis Line, Kids Help Phone, 211, and 911.

Summary of Recommendations

8.1. List of Recommendations

The *IICPA* presents an important step in preventing and responding to the harms of cyberbullying and non-consensual intimate image sharing. Awareness, accessibility, inclusion, and collaboration are essential to ensure that those experiencing these issues are getting the support services they need. This review of the *IICPA* has yielded 12 recommendations:

1. **Build in methods to assess technological advancements, online trends, and opportunities for collaboration with stakeholders to enable continuous process improvements within CyberScan.**
2. **Increase knowledge of the *IICPA* and CyberScan through presentations and public awareness campaigns, including targeted delivery methods for various demographics.**
3. **Clearly state potential consequences of violating the *IICPA* in awareness campaigns to discourage cyberbullying and non-consensual intimate image sharing and encourage victims to seek support.**
4. **Clarify CyberScan access points by developing and publicizing clear parameters, including hours of operation, services offered, and communication timelines while ensuring CyberScan services are accessible.**
5. **Require CyberScan staff to complete training on trauma-informed and restorative approaches when working with victims.**
6. **Develop a centralized, trauma-informed intake process to reduce the risk of re-victimization.**
7. **Review CyberScan service delivery through an Equity, Diversity, and Inclusion lens; monitor and integrate inclusive language to ensure program is accessible and inclusive.**
8. **Work with law enforcement stakeholders to build stronger referral pathways for victims who are experiencing cyberbullying and non-consensual intimate image sharing.**
9. **Review CyberScan services using a victim-centered lens to determine where CyberScan fits on the continuum of victim support offered by government, community organizations, and law enforcement. Determine if, as a result of the above-noted review, a realignment of service provision is required to support the use of a victim-centered approach and connection to support services.**

10. **Work with Department of Education and Early Childhood Development and Regional Centres for Education to learn what support may be needed for children and youth experiencing cyberbullying and/or non-consensual sharing of intimate images, their families, and school staff.**
11. **Review CyberScan services using a victim-centered lens to ensure victims are supported by caseworkers as they navigate pathways to resolution.**
12. **Develop clear pathways for legal and mental health services for victims of cyberbullying and non-consensual intimate image sharing; include contact information for immediate crisis support in CyberScan communications.**

8.2. Next Steps

To ensure this review has a positive impact on the effectiveness of the *IICPA* and its implementation, the following recommendations have been determined to be priorities. Any financial considerations have been included here.

1) *Develop clear pathways for legal and mental health services for victims of cyberbullying and non-consensual intimate image sharing; include contact information for immediate crisis support in CyberScan communications.*

This recommendation will include collaboration between CyberScan staff and Communications Nova Scotia to ensure that the website and related communication materials include contact information for immediate crisis support to ensure that victims who may be vulnerable have clear pathways for support 24 hours a day, 7 days a week. Website and communication materials can be developed to include additional legal and mental health supports and services. This recommendation can be achieved with existing departmental resources.

2) *Clarify CyberScan access points by developing and publicizing clear parameters,including hours of operation, services offered, and communication timelines while ensuring CyberScan services are accessible.*

This recommendation will include collaboration among CyberScan staff to outline what available services look like and what victims can expect when reaching out for support. This can include hours of operation, expected timelines for response, and current intake processes. Once determined, staff can work with Service Nova Scotia and Internal Services to post this information on the website and in printed materials in collaboration with Communications Nova Scotia. There is no additional budget required for this recommendation to be achieved.

3) The following recommendations allow for a step-by-step approach to learning how to best support victims who may be experiencing traumatic events.

Require CyberScan staff to complete training on trauma-informed and restorative approaches when working with victims.

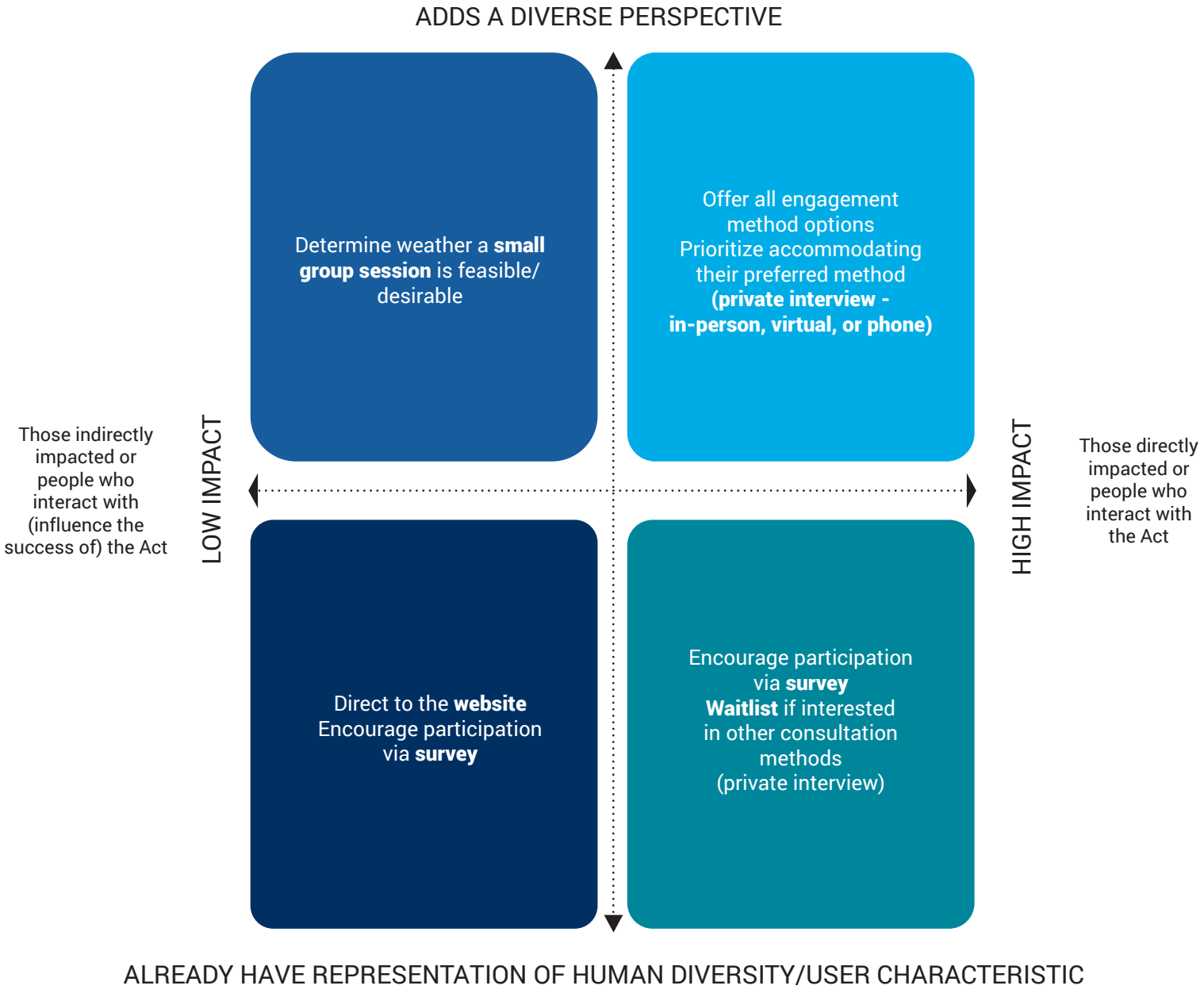
Develop a centralized, trauma-informed intake process to reduce the risk of re-victimization.

The above steps will ensure that CyberScan staff gain valuable insights into trauma-informed approaches and inform a centralized intake process. Financial resources will need to be allocated to complete trauma-informed approaches training for all CyberScan staff.

4) The CyberScan unit has evolved over time under the implementation of both the *Cyber-safety Act* and the *Intimate Images and Cyber-protection Act*. Due to this evolution and the experiences shared during this consultation, it is essential that the unit be reviewed to determine the best fit in terms of services offered to vulnerable persons experiencing cyberbullying and non-consensual sharing of intimate images.

Review CyberScan services using a victim-centered lens to determine where CyberScan fits on the continuum of victim support offered by government, community organizations, and law enforcement. Determine if, as a result of the above-noted review, a realignment of service provision is required to support the use of a victim-centered approach and connection to support services.

Appendix A- Participant Selection Tool



Bibliography

Allen, B. (2019). *Revenge porn and sext crimes: Canada sees more than 5,000 police cases as law marks 5 years*. CBC News. Retrieved from: https://www.cbc.ca/news/canada/saskatchewan/revenge-porn-and-sext-crimes-canada-sees-more-than-5-000-police-cases-as-law-marks-5-years-1.5405118.

Buckner, D. (2020). *Calls to Kids Help Phone have surged. Now some counsellors are making a distress call of their own.* CBC News. Retrieved from: https://www.cbc.ca/news/gopublic/kids-help-phone-toxic-workplace-1.5790617.

Carroll, N., Sadowski, A., Laila, A., Hruska, V., Nixon, M., Ma, D., Haines, J., & On Behalf Of The Guelph Family Health Study (2020). The Impact of COVID-19 on Health Behavior, Stress, Financial and Food Security among Middle to High Income Canadian Families with Young Children. Nutrients, 12(8), 2352. https://doi.org/10.3390/nu12082352.

Crown Prosecution Services. (2017). *Revenge Pornography - Guidelines on prosecuting the offence of disclosing private sexual photographs and films*. GOV.UK. Retrieved from: https://www.cps.gov.uk/legal-guidance/revenge-pornography-guidelines-prosecuting-offence-disclosing-private-sexual.

Department of Justice. (2013). *Comparative International Legislative Responses - Cyberbullying and the Non-consensual Distribution of Intimate Images*. Retrieved from: https://www.justice.gc.ca/eng/rp-pr/other-autre/cndii-cdncii/p5.html.

Department of Justice. (2017). *Cyberbullying and the Non-consensual Distribution of Intimate Images*. Retrieved from: https://www.justice.gc.ca/eng/rp-pr/other-autre/cndii-cdncii/p2.html.

Dinning, B. (2013). Canada: Nova Scotia's "*Cyber-Safety Act*." Borden Ladner Gervais LLP. Retrieved from: https://www.mondaq.com/canada/social-media/271842/nova-scotias-cyber-safety-act.

Dodge, A. (2021). Deleting Digital Harm: A Review of Nova Scotia's CyberScan Unit. Halifax: Dalhousie University.

eSafety Commissioner. (2021). "*Online Safety Act 2021*" *Fact sheet*. eSafety.gov.au. Retrieved from: https://www.esafety.gov.au/sites/default/files/2022-02/OSA%20fact%20sheet%20updated.pdf/.

eSafety Commissioner. (2017). Sending nudes and sexting. esafety.gov.au. Retrieved from: https://www.esafety.gov.au/parents/big-issues/sending-nudes-sexting.

Fraser, D. (2017). *My comments on Nova Scotia's "Intimate Images and Cyber-protection Act."* McInnis Cooper. Retrieved from: https://blog.privacylawyer.ca/2017/10/my-comments-on-nova-scotias-intimate.html.

Government of Canada. (2021). *Sexting and sextortion: what they are and how to deal with them*. Retrieved from: https://www.canada.ca/en/public-safety-canada/campaigns/online-child-sexual-exploitation/resources-for-educators/toolkit-for-youth-aged-15-17/fact-sheet-for-youth-aged-15-17-sexting-and-sextortion.html.

Harris, A. (2020). *Personal Injury: 1st Case under Nova Scotia's "Intimate Images and Cyber-protection Act" Results in Damages of $85,000*. MDW Law. Retrieved from: https://www.mdwlaw.ca/personal-injury-1st-case-under-nova-scotias-intimate-images-and-cyber-protection-act-results-in-damages-of-85000/.

Li, X., Vanderloo, L. M., Keown-Stoneman, C., Cost, K. T., Charach, A., Maguire, J. L., Monga, S., Crosbie, J., Burton, C., Anagnostou, E., Georgiades, S., Nicolson, R., Kelley, E., Ayub, M., Korczak, D. J., & Birken, C. S. (2021). Screen Use and Mental Health Symptoms in Canadian Children and Youth During the COVID-19 Pandemic. JAMA network open, 4(12), e2140875. https://doi.org/10.1001/jamanetworkopen.2021.40875.

Rubin, N., & Taylor, J. (2021). *Liability for online misconduct: do new torts mean increased risk for universities?* Stewart McKelvey. Retrieved from: https://www.stewartmckelvey.com/thought-leadership/liability-for-online-misconduct-do-new-torts-mean-increased-risk-for-universities/.

Seguin, D., Kuenzel, E., Morton, J. B., & Duerden, E. G. (2021). School's out: Parenting stress and screen time use in school-age children during the COVID-19 pandemic. *Journal of affective disorders reports*, 6, 100217. https://doi.org/10.1016/j.jadr.2021.100217.

Sookman, B. (2017). *Worldwide de-indexing order against Google upheld by Supreme Court of Canada*. McCarthy Tetrault. Retrieved from: https://www.mccarthy.ca/en/insights/blogs/snipits/worldwide-de-indexing-order-against-googleupheld-supreme-court-canada.

Statistics Canada. (2021). *Incident-based crime statistics, by detailed violations, Canada, provinces, territories and Census Metropolitan Areas* [Data Table]. Retrieved from: https://www150.statcan.gc.ca/t1/tbl1/en/

Suciu, P. (2021). Cyberbullying Remains Rampant On Social Media. Forbes. Retrieved from: https://www.forbes.com/sites/petersuciu/2021/09/29/cyberbullying-remains-rampant-on-social-media/?sh=3d3352c843c6.

Yousif, N. (2020). *4 million cries for help: Calls to Kids Help Phone soar amid pandemic*. Toronto Star. Retrieved from: https://www.thestar.com/news/gta/2020/12/13/4-million-cries-for-help-calls-to-kids-help-phone-soar-amid-pandemic.html.