DELETING DIGITAL HARM:

A REVIEW OF NOVA SCOTIA'S CYBERSCAN UNIT

ALEXA DODGE, PHD

AUGUST 2021

About the Author: Alexa Dodge is a Hill Postdoctoral Fellow in Law, Justice, & Society at Dalhousie University. She researches legal, restorative, and educational responses to digital forms of sexual violence, harassment, and bullying. This report shares the findings of her current research exploring informal responses to cyberbullying and nonconsensual intimate image distribution through an analysis of Nova Scotia's CyberScan unit.

For questions or media inquiries regarding this report please contact: alexa.dodge@dal.ca

DALHOUSIE
UNIVERSITY

This research was approved by the Dalhousie University Research Ethics Board REB # 2020-5209

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

TABLE OF CONTENTS

DEFINITIONS

Cyberbullying: "An electronic communication, direct or indirect, that causes or is likely to cause harm to another individual's health or well-being where the person responsible for the communication maliciously intended to cause harm to another individual's health or well-being or was reckless with regard to the risk of harm to another individual's health or well-being"[1].

Nonconsensual Intimate Image Distribution: "To publish, transmit, sell, advertise or otherwise distribute" a private nude, semi-nude or sexually explicit image "(i) knowing that the person in the image did not consent to the distribution, or (ii) being reckless as to whether that person consented to the distribution"[2].

CyberScan Unit: The CyberScan unit is a government enforcement unit within the Province of Nova Scotia's Department of Justice. CyberScan agents provide "informal" supports to complainants who are experiencing cyberbullying and nonconsensual intimate image distribution, help complainants navigate civil or criminal law options when applicable, and provide educational presentations on cyberbullying and nonconsensual intimate image distribution to Nova Scotians.[3]

EXECUTIVE SUMMARY & INTRODUCTION

There is growing recognition internationally of the harms associated with cyberbullying and nonconsensual intimate image distribution. In Canada, much of the government response to these issues has focused on legal responses as a core solution (e.g. the federal *Protecting Canadians from Online Crime Act* (2014) and various civil law remedies at the provincial level). Although new criminal and civil law options may lead some to believe that these issues are now adequately addressed, this report finds that legal remedies are often unappealing to many complainants and are unable to address the core issues that underly acts of cyberbullying and nonconsensual distribution. Legal responses do not provide the expedient technological and emotional supports that many victims most desire and they can be counterproductive by bringing additional and extended attention to harmful content. As legal remedies are less widely used and desired than is often assumed, it is necessary to consider what alternatives to traditional legal responses may be available. Therefore, this report analyzes Nova Scotia's CyberScan unit to explore the efficacy of their primarily informal responses to cyberbullying and nonconsensual intimate image distribution.

The CyberScan unit, a government enforcement unit that primarily provides "informal" responses to cyberbullying and nonconsensual intimate image distribution, represents a rare example of a government response to harm that does not require engagement with the legal system. This report provides a detailed description and analysis of the successes and shortcomings of the CyberScan unit as it currently operates. This report will be useful not only for Nova Scotian's seeking to reflect on the accomplishments and room for improvement in responding to cyberbullying and

[1] Intimate Images and Cyber-protection Act, SNS 2017, c 7, para 3(c).
[2] Intimate Images and Cyber-protection Act, SNS 2017, c 7, para 3(d).
[3] https://novascotia.ca/cyberscan/

nonconsensual intimate image distribution in the province, but also for national and international audiences considering implementing alternative responses to these digital harms.

This report details the history of the CyberScan unit (See: History of CyberScan), the types of cases the unit responds to (See: Types of cases responded to), and the various responses the unit offers. As detailed below, the unit was originally created in 2013 as part of the enactment of Nova Scotia's *Cyber-safety Act*. Following the striking down of this act as unconstitutional in 2015, the role of the unit changed to some extent and now operates under the *Intimate Images & Cyber Protection Act* (2017). Under CyberScan's current mandate, CyberScan agents are primarily tasked with providing "informal" supports to complainants who are experiencing cyberbullying and nonconsensual intimate image distribution (See: Most common responses), helping complainants navigate their civil or criminal law options when applicable (See: CyberScan's relationship to civil & criminal justice processes), and providing education and information about cyberbullying and nonconsensual intimate image distribution to Nova Scotians (See: Educational presentations and Communicating CyberScan's role).

While part of CyberScan's mandate is to help victims of cyberbullying or nonconsensual distribution navigate the civil or criminal law responses available to them, this report finds that the vast majority of complainants who contact CyberScan are not interested in engaging in legal processes. Rather, the most common response complainants request is help to remove/report nonconsensually posted intimate images or cyberbullying content from websites or social media platforms. CyberScan agents explain that the expedient removal of harmful content is top of mind for most complainants and, often, no additional action is requested. The second most common resource complainants are looking for is emotional and informational support. CyberScan agents report that it can be a comforting and validating experience for complainants to simply speak with someone who has knowledge of these digital harms and can assure complainants that they are not at fault for having been victimized, that many others have experienced these harms and have found support, and that they do not have to deal with this alone. Much more rarely, complainants are interested in having CyberScan contact the respondent to attempt to stop acts of cyberbullying or nonconsensual distribution by informing respondents of the harm they are causing and/or describing the potential legal consequences of their actions. CyberScan agents report that in almost all cases these informal supports are able to resolve the issue to the complainant's satisfaction and legal processes are not required or desired. The fact that most cases are resolved without recourse to legal remedies (and that most complainants do not desire legal remedies) demonstrates the need for alternatives to legal responses.

While CyberScan is clearly providing vital and in-demand informal responses and support options, this report details several recommendations for improving the unit's responses. Some of the recommendations given in this regard include:

- Provide CyberScan agents with training on best practices for supporting complainants or respondents who are in distress/crisis.
- Provide CyberScan agents with training on best practices for supporting victims in those cases that include acts of sexual violence (e.g. sexualized cyberbullying, nonconsensual intimate image distribution).

- Expand the unit's hours of operation to ensure expedient responses to complainants seeking help to report/remove harmful content, and link to alterative content takedown resources that complainants can access outside of CyberScan's hours of operation.
- Consider hiring additional CyberScan agents to allow for the provision of expedient and holistic responses.
- Re-establish connections with restorative approaches initiatives in the province to provide responses to digital harm that are holistic, forward-focused, inclusive/participatory, and relationship-focused (See: Taking a restorative approach?).
- Ensure CyberScan's website and resource materials accurately explain the range of supports they provide and avoid overemphasizing the legal options that complainants rarely utilize (i.e. better highlight the technological and emotional supports offered).
- Provide resources to help parents/guardians, teachers, and other potential supporters learn best practices for non-judgementally supporting a victim of cyberbullying or nonconsensual intimate image distribution.
- Make the unit more accessible to youth complainants by removing the requirement for youth under the age of 18 to have parental permission to speak with CyberScan.
- Make the unit more accessible to youth complainants by offering options for contacting the unit without having to make a phone call (i.e. offer options to contact the unit through text, live online chat, email, and/or messaging apps).
- Use individual cases of digital harm as a catalyst to consider what systems-level changes are needed to address the broader issues revealed by an individual case (e.g. sexist cyberbullying among a group of teenagers could be used as a catalyst to address sexist beliefs throughout their school's student body and in their school's policies and practices).
- Use CyberScan's experience attempting to report/remove harmful content from various websites and social media platforms to help inform federal initiatives on platform and website responsiveness to takedown requests.

In addition to CyberScan's responses to individual cases of digital harm, the unit is also tasked with providing educational presentations on cyberbullying and nonconsensual intimate image distribution. CyberScan's educational presentations are mainly delivered to youth and take the form of "cyber safety" presentations (See: Educational presentations). The "cyber safety model" of education primarily responsibilizes potential victims to protect their online privacy and to avoid online interactions with strangers, making it largely ineffective at addressing the kind of peer-to-peer cyberbullying and nonconsensual intimate image distribution that is most common among youth. The cyber safety model of education does not address the discriminatory beliefs and relational conflict that often underly acts of cyberbullying and nonconsensual intimate image distribution. Additionally, cyber safety education that focuses primarily on discussions of the victims' role in avoiding harm can be counterproductive by invisibilizing the actions of perpetrators and implying that the culture that supports bullying is natural and unchangeable (Fairbairn et al., 2013; Mishna et al., 2020). Best practices in addressing cyberbullying and nonconsensual intimate image distribution assert that education should be focused on teaching the importance of healthy/ethical relationships, equality/inclusion, consent, and empathy (Fairbairn et al., 2013; Choo, 2015; Johnson, 2016). Therefore, this report provides several recommendations for a major reworking of CyberScan's approach to education, such as:

- Move away from the "cyber safety" model of education and instead seek to address the core discriminatory and relational issues that underly cyberbullying and nonconsensual distribution.
- In collaboration with schools and community organizations, provide ongoing and interactive education on healthy/ethical relationships, equality/inclusion, consent, and empathy.
- Avoid using scare tactic approaches and, instead, help youth feel empowered to make change, seek support, and support others.
- When educating on the topic of nonconsensual intimate image distribution, avoid victim-responsibilizing / anti-sexting approaches that can increase the shaming and blaming of victims. Instead, focus on the importance of consent and respecting the privacy and bodily autonomy of others (See: Education regarding nonconsensual intimate image distribution).
- When educating on the topic of nonconsensual intimate image distribution among youth, avoid framing this act as "child pornography" (See: Labelling youth intimate images as "child pornography").

As detailed in this report, there are several ways in which the CyberScan unit could improve its responses to cyberbullying and nonconsensual intimate image distribution. However, the core supports provided through CyberScan's support line role (i.e. technological and emotional supports for complainants) seem to be a successful and in-demand resource. CyberScan's work in this regard could be used as a model to provide all Canadians with this kind of support line (See: Informing national responses to digital harm). Somewhat comparable services are available in the UK through the Revenge Porn Helpline and in Australia through the national eSafety Commissioner, but Canada does not currently have a national program that provides supports and resources in response to these digital harms. If Canada were to create a national support line and resource hub, the recommendations in this report could also be useful for exploring the kinds of preventative education and restorative responses that a federal program might help nurture at the local level. Both CyberScan's successes and shortfalls offer a useful guide for considering best practices in responding to and preventing the harms of cyberbullying and nonconsensual intimate image distribution.

METHODS

The methodology for this report includes interviews and document analysis. Semi-structured interviews were completed with four CyberScan staff in 2016[4] (one complaints coordinator and three government enforcement agents) and three CyberScan staff in 2020 (one complaints coordinator and two government enforcement agents)[5]. To ensure interviewees could speak openly

[4] One agent was interviewed in 2021 regarding their work with the unit up to and including 2016.

[5] In 2016 the CyberScan unit had 6 staff, but not all staff were available for interviews due to frequent travel for work. In 2020 the CyberScan unit had only 3 staff and all staff members were available for interviews.

about both the successes and challenges that they perceived in the CyberScan approach, interviewees were anonymized and are all referred to as “agents”. Agents are cited using the following anonymous codes:

- CyberScan interviewees from 2016: CS1; CS2; CS3; CS4
- CyberScan interviewees from 2020: CS5; CS6; CS7

Interviews were also conducted in 2021 with two restorative approaches experts that have provided guidance to the CyberScan unit. These restorative approaches experts are referred to using the following anonymous codes:

- Restorative approaches interviewees from 2021: RA1; RA2

The CyberScan website and CyberScan resources were also analyzed. This includes:

- CyberScan’s website at: https://novascotia.ca/cyberscan/
- What you need to know about the Intimate Images and Cyber-Protection Act (PDF)
- Here to help: CyberScan unit (PDF)
- CyberScan’s infographic on Public Outreach Results
- CyberScan’s PowerPoint slides used in educational presentations for youth

HISTORY OF CYBERSCAN

The CyberScan unit was created in 2013 as part of the enactment of Nova Scotia’s *Cyber-safety Act*[6]. The *Cyber-safety Act* was created in response to the tragic death of Rehtaeh Parsons[7] and other high-profile cases[8] in which young people died by suicide in the aftermath of cyberbullying and/or nonconsensual intimate image distribution. The *Cyber-safety Act* created both civil law and informal remedies for cases of cyberbullying and nonconsensual intimate image distribution. It established a tort for cyberbullying, set out the procedure for complainants to apply for a Cyberbullying Protection Order, amended the *Education Act* to ensure that schools address cyberbullying behaviour occurring on or off school property that is disruptive to the school environment, and amended the *Safer Communities and Neighbourhoods Act* to create the CyberScan unit. The CyberScan unit was authorized to investigate complaints of cyberbullying, send warning letters to respondents, apply for Cyberbullying Prevention Orders, provide advice and support to complainants (e.g. through helping to remove cyberbullying content posted online), and attempt to resolve complaints through negotiation or informal agreement. In addition to the responsibilities described in the *Cyber-safety Act*, the CyberScan unit was also tasked with providing educational presentations about cyberbullying to Nova Scotians and acting as a resource for schools responding to incidents of cyberbullying.

[6] Cyber-safety Act, S.N.S. 2013, c. 2.

[7]The death of Nova Scotian teenager Rehtaeh Parsons was the main catalyst for creating the legislation that resulted in the CyberScan Unit (Taylor, 2016). Parsons died by suicide in the aftermath of having an intimate image of her (captured during an alleged sexual assault) nonconsensually distributed and used as fodder for sexist and victim blaming/shaming bullying and harassment by her peers.

[8] Nova Scotia was also at the forefront of discussing issues of digital harm prior to the Rehtaeh Parsons case. As Choo (2015) explains, “after the deaths of teenagers, Jenna Bowers-Bryanton, Courtney Brown and Emily McNamara in 2011, the provincial government created a task force to look into the prevalence of cyberbullying” (p. 68).

In 2015 the *Cyber-safety Act* was struck down by the Supreme Court of Nova Scotia. In *Crouch v Snell* (2015), the *Cyber-safety Act* was found unconstitutional based on sections 2(b) (Freedom of expression) and 7 (Life, liberty, and security of the person) of the *Charter*. In his decision, Justice McDougall referred to the *Act* as "a colossal failure" [9]. A core issue was the overly broad definition of cyberbullying provided in the *Cyber-safety Act,* though other important issues were also detailed by the court (See: Taylor, 2016). David Fraser, the privacy lawyer who challenged the *Act,* was happy to see this particular legislation struck down as he asserts: "I consistently heard from and about people whose political or legitimate *Charter*-protected speech was removed from the internet because members of CyberScan bullied the people into removing it under threat of unspecified 'legal action' that could include removing their internet access" (Fraser, 2017). While the civil law and investigative powers of CyberScan were immediately removed by the striking down of this legislation, the CyberScan unit remained partially active during this time as they were able to continue providing educational presentations and could provide complainants with information (e.g. instructions on how to report a nonconsensually distributed intimate image to a social media company, contact information for counselling in their community).

In 2018 a redrafted version of the *Act,* with a narrower definition of cyberbullying and explicit reference to nonconsensual intimate image distribution, came into force as the *Intimate Images & Cyber Protection Act* (2017)[10]. While this current legislation still allows complainants to apply for civil law remedies through a Cyber-Protection Order[11], CyberScan staff can no longer apply for orders on behalf of complainants and the CyberScan unit is no longer tasked with investigative powers or the authority to send formal warning letters. Rather, the new CyberScan mandate focuses even more explicitly than the original mandate on providing informal resolutions and victim supports. The new mandate under the *Intimate Images & Cyber Protection Act* describes the following role for CyberScan: "(a) provide public information and education regarding harmful on-line conduct; (b) advise public bodies on policies for online safety and conduct; (c) provide support and assistance to victims of intimate image distribution without consent and cyber-bullying; (d) provide information to victims of intimate image distribution without consent and cyber-bullying respecting the criminal justice system and proceedings under this Act; (e) provide information to victims of intimate image distribution without consent and cyber-bullying respecting contacting police; (f) provide voluntary dispute-resolution services, including advice, negotiation, mediation and restorative justice approaches in respect of harmful on-line conduct; and (g) provide such other services, exercise such other powers and authorities and perform such other duties as may be prescribed by the regulations"[12].

Although CyberScan's powers are much more limited under the current *Intimate Images & Cyber Protection Act* than under their original mandate, the unit's work in practice has not changed as drastically as might be assumed. From its inception to the present day the CyberScan unit has primarily provided informal responses/supports and educational presentations. Despite this, most scholarly and media attention has focused on CyberScan's (no longer active) powers regarding

[9] Crouch v. Snell, 2015 NSSC 340, para 165.

[10] Intimate Images and Cyber-protection Act, SNS 2017, c 7.

[11] Complainants can apply for a Cyber-protection Order to, for instance, order a respondent to remove cyberbullying posts and forbid the respondent from contacting the complainant.

[12] Intimate Images and Cyber-protection Act, SNS 2017, c 7, para 12.

civil orders and formal warning letters and little attention has been paid to their informal and educational responses. This report provides a more fulsome understanding of CyberScan's approach by detailing the unit's relationship to civil and criminal law processes as well as the unit's primarily informal and educational responses.

TAKING A RESTORATIVE APPROACH?

Provincial Minister of Justice Mark Furey has stated that CyberScan uses a "restorative approach" in its responses to cyberbullying and nonconsensual intimate image distribution. In 2017 he stated that the province will "continue to help victims with restorative approaches through the CyberScan Unit"[13] and in 2020 he stated that CyberScan applies a "restorative justice methodology"[14]. As the *Intimate Images & Cyber Protection Act* (2017) came into force, provincial politicians[15] and the director of CyberScan also highlighted the use of restorative approaches (Tutton, 2018). *Despite these expressions that CyberScan takes a restorative approach, members of the CyberScan unit themselves do not recall having received directives or resources to work restoratively and said they would not refer to their current response as taking a restorative approach (CS5, CS6).* There seems to be a disconnect between the government's stated intention in this regard and the response provided in practice. One of the restorative approaches experts interviewed for this report suggested that this disconnect could be due to a misunderstanding of what it means to take a restorative approach: "There seems to be an understanding expressed by the government that because CyberScan isn't criminal or punitive focused that they must be restorative, rather than robustly thinking of a restorative approach as a relational approach that looks at the contexts, causes, and circumstances [surrounding a harmful act]" (RA2). Based on the robust restorative approaches that have been championed in the province of Nova Scotia, responses that are called restorative might be expected to be grounded in the following guiding principles: relationship focused; inclusive and participatory; comprehensive/holistic; and forward-focused (RA1).

Although CyberScan does not seem to offer a robust restorative approach in practice, attempts were made in the early stages of envisioning the CyberScan unit to meaningfully connect CyberScan into ongoing restorative initiatives in the province. Most notably, several experts in restorative approaches pushed for CyberScan's work to align with the restorative response to bullying that was already implemented in many Nova Scotian schools (RA2). These experts argued that responses to "cyberbullying" should align with existing restorative responses to "offline" bullying because "cyberbullying is not something completely different from [offline bullying]" (RA2). Both bullying and cyberbullying, they asserted, generally have relational issues at their core and any strict distinction between the two creates a "false divide" that does not reflect the lived reality for "kids [who] carry their devises all the time" (RA2). This assertion is supported by research that has found that young people, like many adults, now understand their "online" and "offline" lives as seamlessly integrated (Boyd, 2014) and that "cyber" and "offline" forms of bullying are significantly interrelated (Mishna & Van Wert, 2015). This early push for CyberScan to take a restorative approach resulted in a professional development day for school principals aimed at bringing CyberScan's response to cyberbullying into harmony with the significant

[13] Nova Scotia, Legislative Assembly, *Hansard*, 63rd Leg, 1st Sess, No 27 (26 October 2017) at 1828-9.

[14] Nova Scotia, Subcommittee of the Whole on Supply, *Hansard* (9 March 2020).

[15] Nova Scotia, Legislative Assembly, *Hansard*, 63rd Leg, 1st Sess, No 27 (12 October 2017).

existing work on bullying in schools. The following is an excerpt from a handout used in the resulting "CyberScan and Schools" professional development day that was held shortly before CyberScan became fully active in September of 2013:

> Schools, government, community agencies, students and families need to build the collaborative relationships essential to addressing and responding to cyberbullying in order to ensure safety and security. The appropriate processes and responses required in the event of cyberbullying may differ on a case-by-case basis depending upon the needs of the students, families, school communities and the range of circumstances and factors involved. The following guiding principles allow the collaboration necessary to craft an appropriate response:
>
> **Relationship Focused:**
>
> - CyberSCAN and schools should understand cyberbullying relationally and respond by examining the relationships involved in and affected by the situation.
> - A response cannot focus on individual students without considering the others involved and affected by the situation including those within the school community, families and wider community.
> - The response will focus on the harm caused to students and others and harmful patterns or structures of relationship; not simply on the breech of rules or laws.
>
> **Inclusive and Participatory:**
>
> - A focus on the relationships between and among those involved requires processes that are inclusive and participatory and culturally proficient.
> - Responses will not only identify who was hurt and who was directly responsible but will inquire who else was impacted or involved and who is essential to responding to the situation and assuring a safe and successful outcome. This can include families, school and community supports and other resources.
>
> **Comprehensive/Holistic:**
>
> - A comprehensive and holistic approach to understanding a cyberbullying incident means considering the context and causes along with the broad ranging effects related to an incident.
>
> **Forward-focused:**
>
> - Responses will approach cyberbullying in a problem-solving and solution focused way. They will focus on understanding what happened including the context, causes and contributing factors of cyberbullying and on determining the appropriate response to ensure that it does not continue.
>
> The focus will be on facilitating and supporting parties to understand and take appropriate responsibility for their actions, address the harmful effects of their actions and commit to a plan to ensure safe and respectful relationships in future.

The above document demonstrates that, when the unit was first being envisioned, there were initial attempts to connect CyberScan into the network of people taking a restorative approach in Nova Scotia. Despite this early work, CyberScan agents interviewed in both 2016 and 2020 did not describe receiving directives, training/professional development, or resources related to providing a robust restorative approach and did not describe their approach as restorative. Those working under the original CyberScan legislation did describe working closely with school principals to respond to cases among youth which, considering the work on restorative approaches being taken in many schools at that time, may have resulted in agents working restoratively in some ways. However, as described in more detail below (See: School-based responses to youth complainants & respondents), CyberScan agents' responses to cases in schools do not seem to follow restorative principles and, rather, seem to often rely on legal warnings and "cyber safety" presentations[16] that do not address the relational conflict or discriminatory beliefs that are at the core of many acts of cyberbullying and nonconsensual distribution.

Agents in 2020 said that, although CyberScan itself does not necessarily take a restorative approach, the Community Justice Society has recently invited CyberScan agents to participate in a few restorative justice responses to cases involving aspects of cyberbullying. Their role in these processes has involved "trying to get [the perpetrator] to think about how their online behaviour can really impact people" and, at times, providing a "one-on-one educational session with the youth to talk about online behaviour" (CS5). This is one way that CyberScan has recently made some connection with the restorative justice processes occurring in Nova Scotia; However, there are much broader ways that CyberScan could link into restorative approaches in the province. As one of the restorative approaches experts explained in terms of restorative responses in schools:

> "Some people think that unless you bring [the victim and perpetrator] together in a circle, you didn't take a restorative approach. But you can take a restorative approach [while having] very few circles. It's not one particular process that makes an approach restorative, but rather it is about taking that lens that asks 'What is going on in the background here? Stop that behaviour please because it's harmful, but tell us what is actually going on.' […] We have to debunk the myth that taking a restorative approach to cyberbullying would mean 'Oh we will just bring in the victim and the perpetrator and we're going to put them in a circle', but rather it looks like asking 'What is going on here? How do we invite participants into this process in a safe way? […] How do you bring in the caregivers of the alleged perpetrator […] in a way that they understand that we are not just looking for a punitive response here, but we are looking to have your child come in and participate in a process to respond to something that is having very serious impacts on somebody else?'" (RA1)

Although CyberScan does not currently work in a particularly restorative manner, there are several reasons to believe that this would be a useful direction to move toward. CyberScan agents described that the vast majority of cases they respond to involve complainants and respondents who are known to each other, primarily as schoolmates, (ex)friends, (ex)partners, work colleagues, or neighbours (CS4, CS5); Therefore, the relationship focused responses offered by restorative approaches could provide appropriate tools for addressing the impacts on relationships that result from digital harms. *In addition to the relevance of relationship focused responses, restorative approaches are also useful because they seek to address the systems-level issues that influence acts of cyberbullying and nonconsensual distribution.* For instance, if an act of cyberbullying involved sexist comments, a restorative approach would seek to address not just the ways sexist beliefs negatively impacted the relationships between the particular youths involved, but would also look at how the school as an institution is normalizing gender inequality. One of the restorative approaches experts explained how a school culture might send the message that gender inequality is acceptable by, for instance, emphasizing male sports over female sports: "If we are structuring [our sports funding] around gender than we are clearly signaling that girls and boys are unequal.

[16] As discussed further in the section on Educational presentations, these presentations do not seem to engage youth in discussion about the rights of others, diversity, consent, or healthy relationships. Rather, these presentations focus primarily on teaching potential victims how to secure their online privacy.

So with this approach […] you need to be thinking about all of what is happening in your building" (RA1). This interviewee explained that it is often necessary to respond expediently to cases to immediately stop the initial harm (e.g. immediately stopping the spread of nonconsensually distributed intimate images), but those responding must then be "willing to sit down and say 'What the heck is going on here relationally? How are things structured here so that that person thought that was a tool that they ought to be able to use without consequences?'" (RA1). In this way, individual moments of harm become catalysts for asking broader questions, such as: "What needs to change in this building? What do we learn from this situation? [Do we need to change] a policy or practice in the building? What different conversations do we need to be having with our students?" (RA1). This approach holds individuals "to account in a meaningful way" while also seeking to "look at the collective responsibility for an incident" (RA1).

Restorative responses are necessary to account for and address the relational issues, discriminatory beliefs, policies, and practices that fuel and aggravate the harms associated with cyberbullying and nonconsensual intimate image distribution. Evidencing this, restorative responses were a core recommendation of the Standing Senate Committee on Human Rights' report *Cyberbullying Hurts: Respect for Rights in the Digital Age* (2012). Recognizing the importance of restorative approaches, this report will consistently reflect on how CyberScan's responses might better connect with the robust restorative principles and resources developed in Nova Scotia. There are certainly ample opportunities for CyberScan to "consider [a restorative] approach to their work and to be a catalyst to building those kinds of responses" (RA2). Through building relationships with and working alongside those in Nova Scotia who are part of an "ecosystem of restorative supports", CyberScan could access "supports to work in more holistic, integrated ways with a really robust set of resources and experiences" (RA2). The new Restorative Research, Innovation and Education Lab could provide a first contact to help CyberScan reconnect with those working restoratively in the province. Engagement with restorative approaches will not involve finding some new "perfect solution" for CyberScan to utilize, rather it will help CyberScan to continuously consider opportunities to improve their responses (RA2).

> *Recommendation #1: Re-establish CyberScan's connection to Nova Scotia's network of restorative approaches initiatives in schools and communities.*

COMMUNICATING CYBERSCAN'S ROLE

All CyberScan agents reported that CyberScan responds to the vast majority of cases through "informal responses" (i.e. responses that do not involve any use of laws or interaction with the justice system). In rare cases that are not resolved informally, agents working under the *Cyber-safety Act* (2013) had the power to send formal warning letters to respondents and to apply for civil court orders on behalf of complainants, while agents working under the *Intimate Images and Cyber-protection Act* (2017) no longer have these powers (See: Use of Civil Court Orders). While these changes in terms of formal responses are important in some cases, they are not as impactful to CyberScan's work as might be assumed because the unit has always provided informal responses to the vast majority of their cases. By far the most common responses that CyberScan agents provide, and that complainants are looking for, are technological and emotional support (See: Most common responses). Much more rarely, agents attempt to resolve issues by contacting respondents to attempt to stop cyberbullying or nonconsensual distribution by explaining the harm the respondent is causing and/or the potential legal consequences of their actions. Even more rarely, CyberScan helps complainants navigate their civil or criminal law options. CyberScan agents consistently explained that most complainants do not want the respondent contacted and even fewer want to initiate a legal response. *Although CyberScan's most in-demand responses are technological and emotional support for complainants, these supports are often not mentioned when communicating CyberScan's role to the public.* For instance, the CyberScan website currently describes CyberScan's resources in the following way: "CyberScan staff can help victims find a solution to a dispute involving cyber-bullying or the sharing of intimate images. They can contact the person who shared the images or cyberbullied the victim to try to resolve the matter informally using dispute resolution, including advice, negotiation, mediation and restorative practices. […] CyberScan can also help victims navigate the justice system and understand their options".[17] *This explanation does not mention emotional support and help with content takedown, and rather focuses on the much more rarely desired options of contacting respondents and engaging the justice system.* While information on rarely used options should certainly be included as they will be useful to a small number of complainants, the current framing of the unit's role could discourage those who are not looking to engage the respondent or begin a legal process from contacting CyberScan. *The above quote also mentions that respondents can be engaged through "mediation and restorative practices", yet CyberScan agents in 2020 report that they have never convened a victim-offender mediation session and that they would not describe the unit as engaging in restorative practices*.

When explaining how CyberScan can help in the document What you Need to Know about the Intimate Images and Cyber-protection Act, there is some mention of providing general "support" to complainants; However, help with content takedown is still not mentioned and the emphasis continues to be on responses that engage respondents or utilize civil law. This is demonstrated in the following section from this document: "CyberScan staff can contact the person who distributed the intimate images without consent or who engaged in cyberbullying to explain the process and try to solve the matter informally using restorative practices or other approaches. They can also help you to navigate the justice system, help you understand your options, offer you support, and try to solve the matter informally using restorative practices or other approaches"[18]. The second document linked to on CyberScan's website, titled Here to Help: CyberScan Unit also places a great deal of emphasis on civil law options. For instance, rather than describing some of the ways that CyberScan can provide immediate emotional and technological supports, this document says to call CyberScan to "learn how to apply for a court order or for more information on additional supports"[19]. This document describes the informal options available saying "CyberScan will seek to resolve the matter informally using restorative practices or other approaches"[20]. *CyberScan's website and documents should be updated to speak more fully and accurately to the reality of what CyberScan offers in terms of responses (e.g. clarify what kinds of "mediation and restorative practices", if any, they offer) and to highlight their most in-demand supports (e.g. support in reporting/removing harmful content and emotional support).*

[17] *novascotia.ca/cyberscan*

[18] What you need to know about the Intimate Images and Cyber-Protection Act (PDF), p.3.

[19] Here to help: CyberScan unit (PDF), p.4.

[20] Here to help: CyberScan unit (PDF), p.2.

Considering CyberScan's mandate to provide education on cyberbullying and nonconsensual intimate image distribution, their website should also be updated to provide links to useful educational resources on these issues. CyberScan agents expressed that they would like to have additional resources to make their website more of an educational and informational hub, however they do not feel that they currently have the capacity to do such work (the unit currently operates with half the staff of the original CyberScan unit). One agent suggested that, with more capacity, they would like to provide comprehensive and regularly updated resources akin to those provided on the website for Australia's eSafety Commissioner (CS5). Although this kind of robust educational hub would require more resources, CyberScan's site could easily be updated to link to existing Canadian organizations that provide comprehensive and evidence-informed educational and support resources. For instance, the MediaSmarts[21] website provides extensive information for youth, parents, and teachers on best practices for education about and support in response to cyberbullying and nonconsensual intimate image distribution. If CyberScan were to develop a more robust educational approach as discussed further below (See: Educational presentations) their website could also communicate the ways that agents could help interested parties to craft educational workshops or resources specific to their school or community's needs.

> *Recommendation #2: CyberScan's website and materials should be updated to accurately reflect the responses they offer and to highlight the options that complainants are most often seeking.*
>
> *Recommendation #3: The CyberScan website should link to comprehensive and evidence-informed educational and support resources on the issues of cyberbullying and nonconsensual intimate image distribution.*

TYPES OF CASES RESPONDED TO

This section provides an overview of the kinds of cases CyberScan responds to. The first subsection describes the demographics of complainants and respondents and the relationship between complainants and respondents in CyberScan cases. The second subsection describes the number of cases CyberScan responds to. And the third subsection describes the types of digital harm CyberScan responds to.

COMPLAINANT & RESPONDENT DEMOGRAPHICS

Because the CyberScan unit emerged in response to high-profile cases of cyberbullying and/or nonconsensual intimate image distribution among young people, it is often assumed that the unit responds primarily to youth cases. However, in both 2016 and 2020 agents reported that *the majority of CyberScan cases involve adult complainants and respondents*[22] (CS2, CS7). In terms

[21] MediaSmarts is a Canadian not-for-profit charitable organization for digital and media literacy.

[22] It is not entirely clear why this is, it could be that youth are less likely to report the harms they experience, are more likely to access supports through family/school, or are less likely to contact CyberScan because the unit can only be

of the gender of complainants, agents in both 2016 and 2020 reported that *most complainants are women/girls* (CS2, CS3, CS7). Rough statistics kept by CyberScan from July 5th, 2018 to November 5th, 2020 show that 56% of complainants are female and 24% are male, with the remaining cases being unrecorded for various reasons (CS7). In terms of the gender of respondents, *women/girls are also somewhat more likely to be respondents.* Based on rough statistics kept by CyberScan from July 5th, 2018 to November 5th, 2020, 38% of respondents are female and around 26% are male, with the remaining cases being unrecorded for various reasons (CS7). *Unfortunately, CyberScan does not currently keep statistics on the demographics of complainants and respondents beyond age and gender.* An agent in 2020 expressed that such data should be collected "because with the cyberbullying you need to identify if there are target groups that are the victims of the cyberbullying. But unfortunately, the system is just not designed to capture that information" (CS7). Research shows that people who are LGBTQ+, Indigenous, racialized, and/or disabled can be disproportionately impacted by cyberbullying and nonconsensual intimate image distribution (Henry et al., 2017; Mishna & Van Wert, 2015); Therefore, CyberScan should consider keeping more detailed demographic data to ensure they are capturing the full picture of digital harm in Nova Scotia and are crafting appropriate resources and responses.

In terms of the relationship between complainants and respondents, in both 2016 and 2020 agents reported that most complainants and respondents are people known to each other rather than anonymous harassers. A 2016 agent explained that it was rare to receive a complaint where the respondent was unknown, "the vast majority of our cases are the peer-to-peer kind of cyberbullying where they are known to each other" (CS4). Agents in 2016 reported that many of their adult cases involve harm being committed in the context of the breakdown of an intimate relationship (CS1). As one 2016 agent explained, "I mean a lot of the adult ones we dealt with were domestic types in the sense of a separation or a break-up, some of them were even over child custody type of stuff, things like that. A lot of adult cases it was nonconsensual image distribution or […] the threat of sending something like that out" (CS2). In 2020 agents explained that cases now seem to somewhat less often involve intimate partners and more often involve "adult neighbours, friends that have fallen out, etcetera" (CS7). The fact that most cases involve complainants and respondents who are known to each other provides important information for the kinds of responses and education that are required.

Recommendation #4: CyberScan should begin recording more detailed demographic data to ensure the unit understands, and appropriately responds to, those populations that are disproportionately impacted by cyberbullying and nonconsensual intimate image distribution.

contacted by phone and because youth require parental permission to speak with a CyberScan agent (See: Emotional support & information).

NUMBER OF CASES RESPONDED TO

During the 2 years and 4 months (September 2013-December 2015) that CyberScan was fully active under the original Cyber-safety Act, CyberScan staff responded to over 800 complaints (CS1). CyberScan staff described struggling to deal with the high call volumes they received during this time period: "[one of the most challenging parts of the job is dealing with] the sheer volume of cases, the very fast pace needed to keep up with it. So could be a good day where you'd have just maybe 10-12 calls a day or could be a day where you could receive 18 calls in one day" (CS1). *Agents in 2020 reported responding to a much smaller number of cases under the Intimate Images and Cyber-protection Act, with 385 files opened between July 5th, 2018 and November 5th, 2020.* CyberScan staff attributed the drop in cases as, in part, due to less public awareness of CyberScan than was the case when the unit was first created: "when [the new legislation] came out in 2018 it was more of a soft launch. There was no big media blitz like there was under the original legislation" (CS5). Another staff member likewise explained,

> "It's a constant struggle trying to get the word out that we exist and that we are here as a resource. You know there are limited budgets for advertising I guess […]. We target schools, make physical brochures, and then do outreach work sending out our website […]. When the legislation was rolled out the communication department tried to [get the word out] and we had like videos made to be released on social media… but I don't know how popular that all has been…usually when [I ask how people heard about us] they'll say either the police have referred them […] or it will be 'Oh a friend used you or I just researched online and came across your website.' And sometimes they will ask 'Are you a service for adults as well as youth?', so I've been asked that before and lots of other things" (CS7)

These comments reveal the need for further, or new types of, public outreach to spread the word that the CyberScan unit exists and that it has resources for both youth and adults. This, along with other issues in clearly communicating the resources CyberScan provides (See: Communicating CyberScan's role), could be resulting in lower numbers of complaints to the unit. In the interest of creating wider public knowledge and use of the unit, it may also be worth considering renaming the CyberScan unit, as the name "CyberScan" does not clearly communicate anything about what the unit does to the average citizen. The unit might gain more immediate recognition if it were named something like "Cyberbullying Helpline", "Cyberbullying & Nonconsensual Intimate Image Distribution Helpline", or "Cyberbullying & Revenge Porn[23] Helpline".

> *Recommendation #5: Create a stronger public outreach campaign and online presence to ensure that the public is aware of what CyberScan is, who the unit can support, and what resources the unit offers.*
>
> *Recommendation #6: Consider renaming "CyberScan" to ensure that the unit's name easily communicates the role of the unit to the public.*

[23] Although many scholars recommend avoiding the term "revenge porn", and instead using "nonconsensual intimate image distribution" or "nonconsensual pornography", it is worth considering which term is most likely to be familiar to the public and is most likely to be entered as a search term when seeking support. The United Kingdom, for instance, has selected "Revenge Porn Helpline" as the name for their support line for victims of nonconsensual intimate image distribution.

TYPES OF DIGITAL HARM

Based on rough data[24] kept by CyberScan from July 5th, 2018 to November 5th, 2020, an agent reported that approximately *70% of the cases CyberScan responded to were cyberbullying cases, 7% of cases included both cyberbullying and nonconsensual intimate image distribution, 5% of cases included only nonconsensual distribution, and the remaining cases were not categorized because they were referred from other agencies* (CS7). In terms of the types of cyberbullying that occurred during this same period, rough estimates indicate that approximately *29% of cyberbullying cases included "nasty comments and name calling"; 20% involved "threats, intimidation, or menacing comments"; 17% involved "false allegations"; 13% involved "impersonation accounts"; and 12% involved "unwanted contact and harassment"*[25] (CS7).

In addition to noting various types of acts such as "name-calling", CyberScan should consider also documenting the types of discrimination that likely underly many of their cases. *When simply logging types of harm such as "name calling" without noting whether it was, for instance, homophobic, sexist, or racist name calling, trends in systemic discrimination—or what Mishna & Van Wert (2015) call "bias-based cyberbullying"—cannot be revealed or addressed.* As discussed further in the below section on education (See: Educational presentations) and the above section on restorative approaches (See: Taking a restorative approach?), CyberScan should ensure that their work is alive to the discriminatory beliefs that often underly the most harmful acts of cyberbullying and nonconsensual distribution. If CyberScan began to track for forms of discrimination they could, for instance, find a pattern of homophobic bullying among youth and use this as a catalyst to work with schools on cocreating a plan to counter homophobia.

The rough estimates above demonstrate that the CyberScan unit responds to a variety of digital harms. Some examples of specific acts that CyberScan interviewees described responding to are listed below.

Agents in 2016 provided the following examples of types of cases they respond to:

- An ex-partner distributing intimate images without consent following a breakup (CS2).
- A young person nonconsensually distributing intimate images of a friend (CS2).
- An ex-partner creating fake social media accounts to repeatedly contact and threaten their ex-partner (CS2).
- An ex-partner using social media to continually post offensive comments about their ex-partner (CS4).
- A young person posting derogatory comments about a peer on social media that other young people use as fodder for further online and offline bullying (CS1).
- A young person screenshotting a private conversation and sharing the screenshot with others leading to widespread online and offline bullying (CS1).
- Teen girls sharing private information about a friend's sex life on social media (CS2, CS1).

[24] The staff member reporting this data stated that all percentages should be interpreted as rough estimates as the data is inputted in a somewhat informal manner and there are sometimes holes/overlaps in data recording (CS7).
[25] These rough percentages do not add up to 100% because some cases are referred from external agencies and are not coded in the system and because a single case can be coded as including multiple types of cyberbullying.

- Posting derogatory comments about individual community members on neighbourhood Facebook groups and encouraging others in the neighbourhood to pile-on by making fun of or bullying the targeted person (CS4).
- Young people creating fake social media profiles of their peers that are used to make fun of them (CS2).

Agents in 2020 provided the following examples of types of cases they respond to:

- Posting "nasty name-calling" about someone on social media (CS5).
- A male partner threatening to post intimate images of their female partner if they breakup with them (CS5).
- An ex-husband nonconsensually distributing intimate images of his ex-wife to try to undermine her reputation during a custody hearing (CS5).
- A young person making a social media account under their school's name (e.g. "Citadel High Confessions") to post rumours about or make fun of individual students (CS5).
- Parents screenshotting bullying messages sent to their child and posting the screenshot on social media to encourage adults to publicly shame the bullying child (CS5).
- Young people creating a shared group chat for their class but leaving out select peers that are made fun of in the chat (CS5).
- Posting private information, images, and/or rumours about someone on public websites designed specifically for anonymous rumour posting and reputational harm (CS6).

These examples help to further demonstrate the various types of cases that CyberScan is tasked with responding to.

> *Recommendation #7: Begin tracking forms of systemic discrimination reported to CyberScan to ensure the unit's work at the individual and systems-level addresses relevant issues of systemic discrimination.*

CYBERSCAN'S RELATIONSHIP TO CIVIL & CRIMINAL JUSTICE PROCESSES

Although the CyberScan unit responds to almost all cases through informal responses, CyberScan sometimes helps complainants navigate civil or criminal law processes. The first subsection below outlines CyberScan's relationship to civil law processes and the ways this has changed since CyberScan's inception. The second subsection outlines the unit's relationship to the criminal justice system. The final subsection discusses how the professional backgrounds and training experiences of some CyberScan agents create additional ties to traditional legal responses.

USE OF CIVIL COURT ORDERS

Under the original *Cyber-safety Act* (2013), CyberScan was able to apply for Cyberbullying Prevention Orders in those cases where informal responses were unsuccessful. *However, even when CyberScan had this power, the vast majority of the unit's cases were responded to without recourse to civil court orders.* CyberScan agents in 2016 reported that the unit used this civil law option in only two[26] cases during the life of the *Cyber-safety Act* (though some members of the public also applied independently for Cyber *Protection* Orders under this legislation) (CS2; CS4). One 2016 agent asserted that CyberScan only applied for court orders in the very few cases where informal responses or warning letters were deemed unsuccessful. In these cases, complainants were deemed to be experiencing "extreme stress and extreme anxiety" and the bullying/harassment was ongoing or had escalated despite informal interventions (CS4). While court orders were rarely used by CyberScan even under the sweeping *Cyber-safety Act*, it is important to note, as privacy lawyer David Fraser has argued, that some CyberScan agents may have used the *threat* of court orders in a manner that resulted in undue limitations on free expression (Fraser, 2017) (See: History of CyberScan).

Under the current Intimate Images and Cyber-protection Act (2017), CyberScan agents can no longer send formal warning letters regarding potential legal action and can no longer apply for court orders on behalf of complainants. Complainants must now navigate and pay for applications for court orders (i.e. Cyber Protection Orders) on their own, which can be a cumbersome and costly process. As one agent described:

> "It's a lot of pressure for somebody to have to go fill out all those forms. If someone is harassing you or whatever, think of all the stress you already have in life, whatever is going on with kids, financially, relationship breakdown, and now maybe you don't have the capacity electronically to do this, or you don't have the money, or a vehicle to get from point a to point b for the courthouse. And now you're responsible to download all this paperwork, fill it out appropriately, and then file it, and then there is a cost[27] to that too" (CS4).

When CyberScan staff were interviewed for this report in November of 2020, they had not supported a single complainant that chose to apply for a court order under the current legislation. Additionally, they knew of only one person who had applied for a court order on their own (this person had not contacted CyberScan before proceeding and the unit only learned of the case through media coverage) (CS5, CS6). Thus, under the current legislation, civil law remedies are even more rarely used and CyberScan has very little relationship to civil law aside from the ability to explain the application process for court orders to complainants that wish to apply on their own. One agent explained the limited role CyberScan now plays saying, "[if a complainant] wants to know a lot about the Cyber Protection Order process we will send them links about what the affidavit process looks like […] and a link to the legislation. […] But again, it doesn't have anything really to do with us… it's a separate process when you are applying to court" (CS5). While CyberScan agents have not yet supported a complainant that has followed through with the court order process, the CyberScan website does include a detailed document titled "What you Need to Know about the Intimate Images and Cyber-protection Act" that could be used by those

[26] Minister of Justice Mark Furey has stated that under the original legislation "CyberScan investigated over 800 cases and, of those, ten cases went to court" (Nova Scotia, Legislative Assembly, *Hansard*, 63rd Leg, 1st Sess, No 27 (12 October 2017) at 1166). It is unclear why exactly Furey cites 10 cases and CyberScan agents cite two, but it is possible that the ten cases mentioned include both those applied for by CyberScan and those applied for by the public independent of CyberScan.

[27] It costs approximately $250 to apply, which can be waived for people below a certain income level who apply for a fee waiver. However, this cost, which is already inaccessible to some, will be much higher if the complainant requires a lawyer.

applying on their own. This document explains the ways a Cyber Protection Order could be useful in terms of having images or content ordered to be removed, potentially receiving monetary damages, forbidding the respondent from contacting the complainant, or ordering dispute-resolution services. This document also explains that the process can be challenging and costly. Although this document is clearly written and could be useful to complainants, the amount of detail provided within it also acts to reveal just how complex and inaccessible the court process can be for the average citizen.

CyberScan agents expressed that the limited support they can now provide for applying for court orders acts as a significant barrier to responding to those rare cases where informal supports are insufficient. One 2020 agent explained that, under the current legislation, CyberScan has responded to about 7 cases in which they believed that informal processes had not resolved the matter and that a complainant might want to apply for a Cyber Protection Order (CS7); However, in each of these cases complainants reportedly did not to move forward with the application because "the court process was too onerous for them to actually want to pursue it" (CS7). The court process was seen as especially onerous in rare cases where the complainant is unaware of the identity of the cyberbully; In such cases, the process involves first applying to reveal the respondent's identity before applying for a court order (CS5; CS7). Therefore, *agents in 2020 expressed that the current legislation should be updated to provide more support for complainants in those rare cases where, despite informal responses, harm is severe and ongoing* (CS5; CS6; CS7). David Fraser, the privacy lawyer who argued that the original legislation was overly broad and violated the rights of accused people, has also expressed concern that the new legislation may have "[swung] the pendulum a little bit too far" by leaving victims to fend for themselves in court or hire a lawyer at significant cost (Palmeter, 2017).

In addition to the challenges of accessing civil remedies, CyberScan agents explained that there are several other reasons that complainants are often uninterested in engaging civil law. For instance, agents explained that there is a risk that going to court will simply bring more attention to the case and thereby result in more people in the community expressing opinions about or bullying the complainant (CS5, CS3, CS7). Although anonymity can be granted to complainants in some cases and is automatically applied to those under 19, in those cases where anonymity is not promised the complainant may worry that a court process will only bring more attention to the rumours, private information, and/or discriminatory content being disseminated about them (CS7). One agent explained that, even if anonymity is granted, complainants in small communities often worry that their identity could still easily be revealed by word of mouth (CS5). As a 2016 agent put it:

> "Complainants definitely [want to keep it informal], especially in small communities. You know, if you can handle this here… it'll go away here. [If you take it to court] the problem can get bigger, there's a fear of further exposure, there's fear of public display, of it becoming a bigger thing than it maybe needed to, you know. Certainly a lot of it was the private sexual information or images for females, especially. So the bigger it may have become, was certainly a problem for them. We did it the right way. I have no doubt about it…. with that informal resolution. […] It's the most efficient way to deal with the social media problem that we're facing for sure." (CS3)

This agent explained that *many complainants see a court process as counterproductive, as it may result in additional and extended attention being given to their nonconsensually distributed intimate images or to the harmful comments being made about them through cyberbullying behaviour.* This agent explained that this might be especially the case for female complainants who have had intimate images or private information/rumours about their sexual lives digitally disseminated. Another reason complainants may not proceed with a court order is that applying for an order is a slow process and the damage may already be done by the time an order can be made (CS7). While civil law remedies have been utilized in a few cases where informal responses were deemed inadequate, *it seems that civil law remedies are rarely more appealing than the informal options offered by CyberScan. Therefore, in addition to considering ways to make civil options more accessible, it is important to adequately resource the CyberScan unit and ensure that the public is aware of the informal options the unit offers.*

> *Recommendation #8: Consider providing additional supports for complainants in those rare cases where civil law remedies are pursued.*
>
> *Recommendation #9: The government of Nova Scotia should continue to fund CyberScan's resources for informal responses as court orders are rarely used and have several limitations. The government should consider whether CyberScan is able to adequately provide the important informal supports they offer with their current number of staff.*

RELATIONSHIP TO CRIMINAL RESPONSES

The CyberScan unit can respond both to acts that rise to a criminal level (e.g. cyberbullying cases that amount to criminal harassment and cases of nonconsensual intimate image distribution) and acts that do not rise to a criminal level. While the unit is sometimes misunderstood as working only to respond to cases that would otherwise not qualify for government response, the CyberScan unit also plays an important role as an alternative option to the often blunt and slow criminal justice process. In Murray Segal's (2015) independent review of the Rehtaeh Parsons case, he speaks to CyberScan's role as a necessary alternative option:

> "The criminal prosecution of individuals should not be the be-all and end-all of solutions. While there will always and should always be a place for the traditional police investigation and criminal prosecutions, which can be valuable tools for reducing crime, we should not lose sight of the fact that they are only one set of tools. We must accept their limitations and embrace alternative solutions. […] In particular, I think of the CyberScan initiative […]. This unit […] will investigate allegations of cyberbullying and intervene if warranted. They have a host of measures at their disposal to stop bullying while, at the same time, raising awareness among cyberbullies and the public." (p. 41)

Evidencing the limitations of typical criminal justice responses and the need for various "sets of tools" to respond to digital harms, CyberScan agents report that most complainants who contact them are interested in accessing informal supports to resolve even criminal level harms in more expedient and victim-centred ways (CS2; CS5; CS6). As discussed further below (See: Most common responses), *most complainants are more interested in receiving expedient technological and emotional/informational support than they are in having the respondent investigated or punished. Considering this, it is important that CyberScan is understood not only as a resource for cases that do not rise to the criminal level, but also as an in-demand alternative response to criminal level cases.*

CyberScan agents seem to vary in the extent to which they promote CyberScan as an alternative option that is available even in cases that rise to a criminal level. At least two CyberScan agents expressed strongly encouraging complainants with criminal level cases to report to police. For instance, an agent in 2016 explained that they tell victims of nonconsensual intimate image distribution that "it's a federal offence and to contact their local policing agency" (CS1). An agent in 2020 described that, although they recognize many complainants do not wish to pursue a criminal response, they still encourage complainants to go to the police if their case involves potentially criminal acts: "obviously if there is a criminal element I will say 'These are criminal offences', and though we have a role as well I will refer them to police, like say 'You really need to go back to the police or make a report to the police'" (CS7). These agents seem to imply that complainants *should* pursue a criminal response when possible, despite the fact that most of the complainants the unit supports are more interested in accessing alternative supports. Recognizing the many reasons particular complainants might have for preferring alterative responses, many other CyberScan agents explained that they describe the various support options available to complainants without implying that complainants *should* go to the police or that the criminal justice process is necessarily the best option. *Although agents seem to vary in the extent to which they encourage complainants to make formal complainants to police, all agents recognized that this option was not desired by most complainants.* As an agent in 2016 described, complainants often see formal criminal justice approaches as unappealing and are more interested in the expedient and informal supports CyberScan can provide:

> "A victim of cyberbullying… a victim of any of this…they just want it to stop. […] I find they don't want to go to court and, you know, keep the attention on this for a long time. No, they want help to get the image down or the content down and get that deleted so that it's not posted again and it stops spreading to others. They want it to stop so they can get on with their lives. And we were able to deliver that for the majority of [victims]. And we'd be able to it quickly." (CS2)

Agents explained that complainants generally do not wish to extend the time and attention paid to the harm they experienced through a criminal process and, when told they can access supports without requiring a formal criminal process, most complainants are eager to address the case informally with CyberScan. One 2020 agent explained that *some complainants also prefer informal responses because they do not wish to criminalize the respondent*. Especially in cases where a complainant is or was in a close relationship with the respondent, they often want the respondent to understand the harm they are causing but do not want the respondent criminalized (CS5). This agent provides the example of a complainant who had her intimate image distributed without consent by an ex-partner that was struggling with alcoholism. The complainant wanted the respondent to know that what they did was harmful and to get support to deal with their use of alcohol, but they did not see a criminal response as helpful (CS5). This agent explained that, when considering what response will be most helpful, you have to ask "Is it best to charge them criminally with that? Or is it best to look at the particular incident and kind of learn from it? And especially if the person is remorseful and takes responsibility for it and we can kind of move forward … it's just so much better to go ahead with it that way" (CS5). Echoing CyberScan agents' experiences with complainants in many ways, research on cyberbullying and nonconsensual distribution has also found that legal approaches can be unappealing as they are often lengthy and can extend the life of a conflict (which can be particularly damaging in youth cases), they're largely offender-focused and not responsive to particular victim and community needs, they're punitive-focused and not necessarily designed to help respondent's meaningfully learn and change, and they can result in revictimization due to officials, such as police officers, that may engage in victim blaming/shaming[28] (Choo, 2015; Dodge & Lockhart, 2021; Powell & Henry, 2017; Shariff & DeMartini, 2015).

In cases where complainants do decide to report to police, CyberScan sometimes stays involved with the file in a victim support role (i.e. emotional/informational support and help navigating the criminal justice system). An agent in 2016 described performing this role in a case involving nonconsensual intimate image distribution: "The police […] moved forward with criminal charges and then we were kind of a resource or a […] friend I guess. So the victim she did keep in contact with one of the [CyberScan agents] and was able to get advice that she needed […] and, even though we weren't active in the investigation because it was a policing file, she still knew that we were here" (CS1). An agent in 2020 explained that a similar victim support role continues in CyberScan's current form: "We do work in conjunction with police, you know if there is an ongoing police investigation we will say, 'What can we do to assist? What is our role here? How can we help?' It might just be a matter of being the liaison because the complainant is frustrated that they aren't getting any updates and we can say 'Who is the officer?' and just trying to help in whatever way we can" (CS7). These agents described filling some of the victim support needs that are often not adequately provided by the criminal justice system itself. In this way, CyberScan acts as both an alternative to criminal justice responses and as a support to fill gaps in typical criminal justice responses.

CyberScan agents also described sometimes working in a kind of "tech support" role for police officers who often do not have the full technological know-how to respond to cases involving digital harms. When asked if, in their experience, police officers are equipped to respond to cases involving digital technology, one agent in 2016 replied:

> "The difficulty is, in my experience, that police officers are supposed to be […] experts if you will in every area and […] that's difficult unless you have special units or you have ongoing training. […] So a lot of police officers don't have the technical background or understand social media and […] a lot of the frontline members don't know how to preserve accounts for example on Facebook. They don't know how to preserve the evidence legally in order to get an order from a court to get the IP address or whatever. So we educate them for sure, all the time too. They're becoming better with it, because we've been working with them a lot. And we'll assist them if they just want information on 'How do I do this

[28] A recent example of criminal justice responses resulting in victim blaming can be seen in the case of a woman who reported several cases of nonconsensual intimate image distribution perpetrated against Indigenous women to the Nova Scotia RCMP. She reports that she felt the RCMP response engaged in victim blaming by responding that she should tell her friends never to share intimate photos with anyone. This woman states: "We don't need a lecture. It's not our fault that these men put these photos on these websites without our consent" (Reynolds, 2021).

> with Twitter?' or whatever, then we'll walk them through that stuff. […] A lot of the information is available online now through those social media sites, but again it's just very difficult for a person to understand all of these things […]" (CS2).

Another agent in 2016 similarly explained, "I think that my experience tells me that [police officers] are terribly under… not aware of the situation of social media. […] I personally spoke to at least twenty police officers who said to me 'What's this [social media] all about? What am I supposed to do? I don't know what to do. Can you help me? I'm lost here.' That was often the response that I got from the police officers, both the RCMP and the municipal police" (CS3). This agent also explained that some complainants come to CyberScan saying that frontline police officers were completely unable or unwilling to provide assistance because they didn't understand the nature of the digital harm being reported (CS3). One interviewee in 2020 confirmed that CyberScan is still sometimes involved in supporting police officers to understand many aspects of responding to cases involving digital technology (CS7).

> *Recommendation #10: CyberScan's communications with individual complainants and with the general public should explain that the unit is both a resource for dealing with harms that do not rise to the criminal level and an in-demand alternative to criminal justice responses.*
>
> *Recommendation #11: CyberScan should be resourced at a level that recognizes the variety of ways that agents work to address gaps in the traditional criminal justice response.*

TRAINING & PROFESSIONAL BACKGROUND

CyberScan staff mainly have professional backgrounds in policing, corrections, and government enforcement roles. Of the four CyberScan staff interviewed in 2016, one had a professional background in government enforcement, two were ex-police officers, and one had a background in corrections. With CyberScan's mandate being to respond primarily through informal, restorative, and educational approaches, it is surprising that hiring has focused narrowly on those with more traditional criminal justice and enforcement backgrounds. In 2020, CyberScan staff also had professional backgrounds related to policing, corrections, and enforcement; However, these staff described having worked in roles that were more focused on justice advocacy or victim support within these professions, and one staff member also had considerable background experience working with digital forms of harm. Therefore, while there are still gaps in the skillsets that would be needed to provide robust restorative or educational responses, CyberScan staff in 2020 seemed to have more experience to draw from in terms of the support aspect that makes up a large portion of CyberScan's work.

Considering that CyberScan's role is increasingly focused on providing emotional support, assistance with reporting/removing harmful digital content, and providing educational presentations, future hiring choices should consider what gaps in knowledge might be filled by hiring those outside of the worlds of policing, corrections, and enforcement. For example, although education makes up a significant portion of CyberScan's role (See: Educational presentations), CyberScan staff do not feel they have expertise in this area (CS5, CS6). *Future hiring should consider diversifying the backgrounds of staff by adding, for instance, those with experience in youth education, counselling, tech support, and restorative approaches.* As one of the restorative approaches experts commented, "I think [CyberScan] did in some ways hire people interested in different approaches to public safety… but certainly there wasn't a lot of balance on the team in terms of educators, community organizers, facilitators or people who have worked in this [restorative] way. You could imagine hiring kind of a balance of people that could have brought their various skills and helped each other" (RA2). Diverse skillsets could only be a positive addition in terms of CyberScan's mandate to "try to think outside the box [of typical legal approaches] to assist Nova Scotians" (CS6).

In terms of the training provided to CyberScan staff, in both 2016 and 2020 agents described receiving police training courses in online investigation techniques and forensic interviewing. Again, considering their mandate to primarily respond through victim support, restorative approaches, and educational presentations, it is surprising that staff are not provided training in areas such as restorative approaches, best practices for supporting people in distress/crisis, or best practices in educational engagement. Additionally, as CyberScan responds to many cases that include some element of sexual violence (e.g. nonconsensual intimate image distribution or sexualized cyberbullying) or domestic violence (e.g. threats to distribute intimate images if a person ends an abusive relationship or campaigns of online rumour spreading in the aftermath of a breakup), CyberScan agents should receive specific training in how to support victims of sexual and domestic violence. *Although CyberScan staff expressed that they generally felt equipped to respond to cases based on their backgrounds in policing, corrections, and enforcement, it is worth considering how responses could be improved by providing training in areas such as supporting someone in distress/crisis, supporting victims of sexual and domestic violence, and providing education to youth.* In terms of acting on the promise to provide a restorative approach (See: Taking a restorative approach?), the restorative approaches experts interviewed for this report were adamant that, *to truly work restoratively, simply providing training sessions to CyberScan staff will not be enough.* As one of these experts stated, "we cannot teach a restorative approach through a one-day workshop. [….] we have to set up the system and create relationships to be able to work with people who want to work [restoratively]" (RA1). This interviewee felt that government leaders need to refocus on the restorative approach that was imagined during the envisioning of CyberScan and support CyberScan staff in taking this approach (RA1).

Recommendation #12: Future hiring, training, and resourcing for the CyberScan unit should focus on filling gaps in terms of the unit's ability to robustly support people in distress/crisis, support victims of sexual and domestic violence, provide education to youth, provide technological support, and respond restoratively.

MOST COMMON RESPONSES

From its inception, CyberScan has responded to the majority of cases using what agents refer to as "informal" approaches. As detailed in the subsections below, *the most common responses provided by CyberScan include helping complainants to remove/report nonconsensually posted intimate images or cyberbullying content from social media platforms/websites and providing emotional/informational support to complainants (CS7)*. *Much more rarely, CyberScan staff contact the respondent to attempt to have them remove images/posts and stop further bullying by explaining the harm they are causing and/or describing the potential legal impacts of their actions*. In very few cases, CyberScan staff assist complainants with navigating legal options (See: CyberScan's relationship to civil & criminal justice processes). CyberScan staff explained that, above all, their approach is based on meeting the stated needs of complainants: "The main thing when it comes to complainants that call in is [to ask] 'What do you want to see happen? What is it that you are looking for?' Because we have lots of options, but it's about letting them choose, because this is their file" (CS6).

IMAGE/CONTENT TAKEDOWN AND TECHNOLOGICAL KNOW-HOW

Agents in both 2016 and 2020 shared that helping complainants to report/remove harmful social media posts and website content is the most common response they provide. A 2016 agent asserted that "99.9% of [complaints] just want the cyberbullying to stop and the comments to come down" (CS4). Even in cases of nonconsensual intimate image distribution, in which complainants have the clear option to report to police, agents explained that most complainants "just want it to stop, they want the image deleted from the other persons device, that's mainly it. […] Like if a woman is calling and saying, 'I don't want him contacted, I just want that image taken off the web', then we will go on there and find out how to take the image down and offer as much support as we can with that" (CS5). *CyberScan's role in providing technological support is extremely important as agents consistently explained that the main concern of most complainants is to have harmful content removed.* For example, a 2016 agent described a case in which a woman's ex-boyfriend had posted offensive claims about her online and it wasn't until this content was removed that she felt she could go out in public in her small community again and "put her head up and get on with her life" (CS3).

CyberScan can provide technological supports by helping complainants to navigate standard avenues for content reporting/removal (e.g. reporting mechanisms on various social media platforms or requests to delist nonconsensually posted intimate images from Google search results) or by using their "established strong networks […] with social networks like Twitter and Facebook" to expediate this process (CS5). In some cases, content is removed by contacting the respondent to request voluntary removal. As expediency in removing or stopping the spread of cyberbullying content and/or nonconsensually distributed intimate images is often top of mind for victims (Choo, 2015; Segal, 2015; Shariff & DeMartini, 2015), it is vital to offer this kind of support for content reporting and removal. In Murray Segal's (2015) review of the response to the Rehtaeh Parsons case, he praises CyberScan's approach in this regard as one of "the most novel and directly responsive solutions to what was arguably the most time-critical aspect of Rehtaeh's torment: getting ahead of the damaging photograph that was circulating like wild-fire among her peers" (p. 116). An Agent in 2016 expressed that, in cases of nonconsensual intimate image distribution, they were often able to have posts removed quite quickly: "we tell victims, 'we will help you try to get these photos back and we will do it as quickly and as discretely as possible'. […] Our response time is very quick when we do that kind of stuff" (CS2).

CyberScan agents explained that some platforms and websites are very responsive to requests for removal of harmful content; However, content removal is not always straight forward or expedient. Agents explained that certain platforms/websites can be more challenging to work with and certain kinds of content can be more challenging to address. An agent in 2020 explained that, even when working with the dominant social media platforms that can be quite responsive, issues such as fake accounts can be more difficult to expediently remove: "[fake] Instagram accounts seem to be a big thing right now […] and trying to get it taken down is not easy, it's not going well" (CS6). Websites such as "The Dirty", that are devoted solely to posting rumours and bullying/harassing content, can also be much more difficult to deal with. As one agent in 2020 explained, such websites will often refuse to remove offensive content about an individual; However, for those websites based in the United States, CyberScan has had success with having *images* of complainants removed through the use of the Digital Millennium Copyright Act (1998) (CS6). Agents also described that, although they are certainly able to assist more quickly than through formal legal channels, content removal is still sometimes a slower process than they would like it to be. An agent in 2016 explained that "[One of the most challenging aspects of the job] is our inability to have social media companies provide us the closure that we want instantly. […] it's a challenge to get an immediate response" (CS3). An agent in 2020 likewise explained that they "wish there was a quicker way to get posts taken down" (CS5). *Although content cannot always be fully removed or expediently removed, agents described being at least partially successful in most cases and reported that complainants are usually very grateful for any support that can be provided in this regard.*

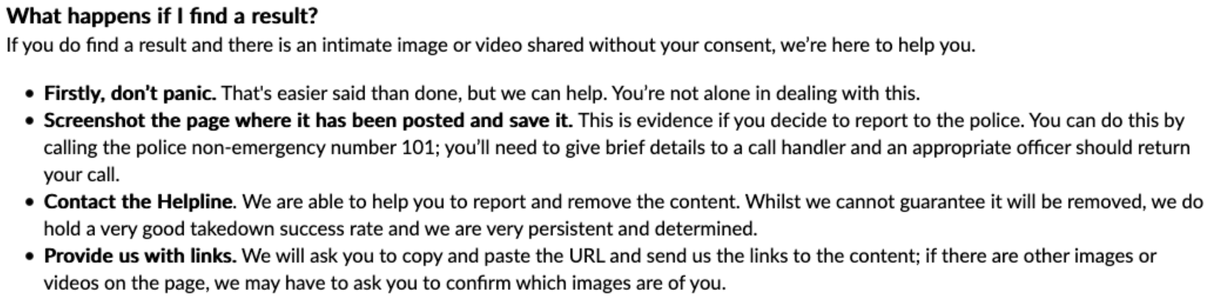
CyberScan's knowledge of the most problematic websites/platforms to work with and the most challenging types of content to remove should be used to inform federal initiatives[29] *that are currently investigating ways to make social media platforms and websites more responsive to requests for removal of harmful content (Khoo, 2021).* Changes already implemented by some social media companies and search engines have shown promise in terms of making content removal easier and more expedient in some cases. Especially regarding nonconsensual intimate image distribution, many social media platforms and search engines (e.g. Google and Bing) have created somewhat more effective reporting options due to activist pressure (Online Removal Guide, 2021). Defining what content should and should not be removed can sometimes be a challenging balance between considerations of harms caused versus freedom of expression (See: Khoo, 2021); However, websites and social media platforms should be able to at least decrease response times to clearly criminal content, such as nonconsensually posted intimate images (Crofts & Lievens, 2018; Khoo, 2021).

While social media platforms and websites are often responsible for slow responses to requests for content removal, an agent in 2020 also described how CyberScan's response can sometimes slow down this process. CyberScan only accepts calls during regular business hours Monday to Friday, which means complainants who call in the evening, on a weekend, or on a holiday will not

[29] https://www.canada.ca/en/canadian-heritage/campaigns/harmful-online-content/technical-paper.html#a3

receive supports for several hours or days: “you know you get the call [from the complainant], it’s not maybe until the next day that you [can respond]. […] technology moves so quick that the damage is already done. […] then even if you report it, it might take a week to be taken down […]. So it’s just that I wish there was a way that… some of the posts are just so harmful to people, even just talking about rumours […] by the time they ever get shutdown the damage is already done” (CS6). *CyberScan’s role in slow response times could be addressed by expanding the unit’s hours and linking to do-it-yourself resources that help individuals learn how to report bullying posts or nonconsensually shared intimate images on various platforms.* Although not all complainants will be able to navigate reporting on their own, links to these resources would certainly be useful for a portion of complainants that are struggling with time-sensitive needs. CyberScan’s website should share links to resources such as Google’s form for reporting intimate images shared without consent[30] and NeedHelpNow.ca’s[31] instructions on how to report content on Snapchat, Instagram, YouTube, or a peer’s phone. International resources, such as Australia’s eSafety Commissioner[32] website, the United Kingdom’s Childline[33] website, and the Cyber Civil Right’s Initiative[34] in the US, provide additional resources on how to report cyberbullying or nonconsensual distribution on platforms such as Twitter, TikTok, WhatsApp, and more. CyberScan could provide links to this kind of do-it-yourself reporting information while also encouraging complainants to contact the support line for additional help during operating hours.

As described above (See: Communicating CyberScan’s role), CyberScan’s website and resources could do a better job of explaining the supports they provide in terms of content reporting and removal. The CyberScan website should highlight this service and provide reassuring messaging to complainants that may be feeling hopeless. As shown in the below image, the UK’s Revenge Porn Helpline[35] provides a useful example of the kind of reassuring messaging that should accompany reporting/removal resources:



What happens if I find a result?

If you do find a result and there is an intimate image or video shared without your consent, we’re here to help you.

- **Firstly, don’t panic.** That's easier said than done, but we can help. You’re not alone in dealing with this.
- **Screenshot the page where it has been posted and save it.** This is evidence if you decide to report to the police. You can do this by calling the police non-emergency number 101; you’ll need to give brief details to a call handler and an appropriate officer should return your call.
- **Contact the Helpline**. We are able to help you to report and remove the content. Whilst we cannot guarantee it will be removed, we do hold a very good takedown success rate and we are very persistent and determined.
- **Provide us with links.** We will ask you to copy and paste the URL and send us the links to the content; if there are other images or videos on the page, we may have to ask you to confirm which images are of you.

It’s important to note the reassuring tone of the above messaging provided by the Revenge Porn Helpline. Although guarantees about image removal cannot be made, the messaging ensures victims that there are supportive resources available to them and that there is hope. Another

[30] https://support.google.com/blogger/answer/7540088?hl=en

[31] Needhelpnow has useful tech know-how resources, however it should be noted that some of their materials have been found to engage in victim blaming/shaming or provide an overemphasis on criminal law: https://needhelpnow.ca/app/en/#

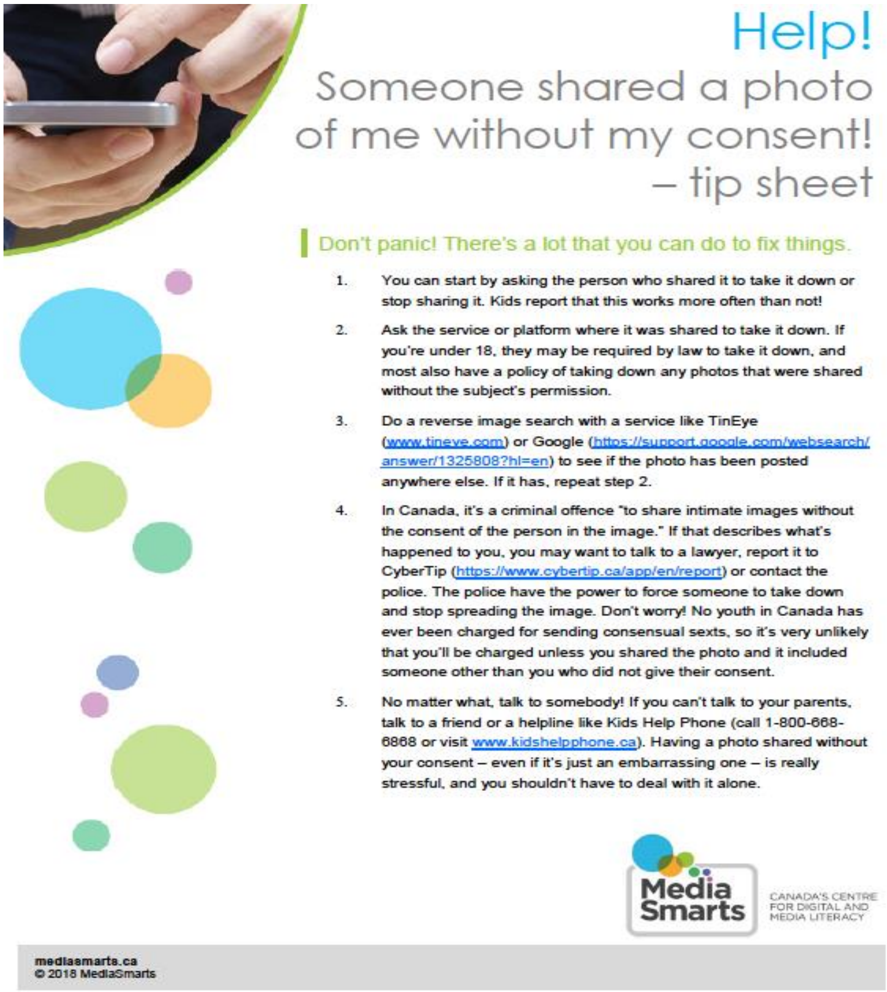
[32] https://www.esafety.gov.au/key-issues/image-based-abuse/take-action/report-to-social-media-website

[33] https://www.childline.org.uk/info-advice/bullying-abuse-safety/types-bullying/bullying-social-media/

[34] https://www.cybercivilrights.org/online-removal/

[35] https://revengepornhelpline.org.uk/

example of how to provide tips for reporting along with reassuring messaging can be seen in the below MediaSmarts resource for Canadian youth:



Help!

Someone shared a photo of me without my consent! – tip sheet

Don't panic! There's a lot that you can do to fix things.

1. You can start by asking the person who shared it to take it down or stop sharing it. Kids report that this works more often than not!
2. Ask the service or platform where it was shared to take it down. If you're under 18, they may be required by law to take it down, and most also have a policy of taking down any photos that were shared without the subject's permission.
3. Do a reverse image search with a service like TinEye (www.tineye.com) or Google (https://support.google.com/websearch/answer/1325808?hl=en) to see if the photo has been posted anywhere else. If it has, repeat step 2.
4. In Canada, it's a criminal offence "to share intimate images without the consent of the person in the image." If that describes what's happened to you, you may want to talk to a lawyer, report it to CyberTip (https://www.cybertip.ca/app/en/report) or contact the police. The police have the power to force someone to take down and stop spreading the image. Don't worry! No youth in Canada has ever been charged for sending consensual sexts, so it's very unlikely that you'll be charged unless you shared the photo and it included someone other than you who did not give their consent.
5. No matter what, talk to somebody! If you can't talk to your parents, talk to a friend or a helpline like Kids Help Phone (call 1-800-668-6868 or visit www.kidshelpphone.ca). Having a photo shared without your consent – even if it's just an embarrassing one – is really stressful, and you shouldn't have to deal with it alone.

Media Smarts

CANADA'S CENTRE FOR DIGITAL AND MEDIA LITERACY

mediasmarts.ca
© 2018 MediaSmarts

Unlike some materials for youth that aggravate anxiety through worst-case-scenario assertions that nonconsensually distributed intimate images will irreparably impact a victim's reputation and future job and school prospects (Angelides, 2013; Dodge, 2021), this resource provides reassurance that there are supports and tools available to alleviate and heal some of the harms being experienced and that a youth does not need to panic. By linking to resources such as these, CyberScan could easily provide more expedient technological support and reassurance to complainants. However, online guides should not replace the ability to get one-on-one support from a CyberScan agent, as several agents asserted that the human connection with complainants can be healing and that many Nova Scotians struggle to understand do-it-yourself instructions due to low levels of technological know-how. One-on-one support also allows agents to determine and support other technological needs. For example, *CyberScan agents often provide complainants with additional technological know-how such as explaining that unwanted contacts can be deleted or blocked on social media platforms*: "part of the job is doing research on what the community guidelines are on say Facebook or something like that and letting the person know about blocking features and deleting, because some people surprisingly still don't know about some of those options, if something happens they don't know you can delete the person or block them" (CS5).

Recommendation #13: CyberScan's knowledge of the most problematic platforms/websites to work with and the most challenging types of content to remove should be used to inform federal initiatives investigating ways to make platforms/websites more responsive to takedown requests.

Recommendation #14: Due to the often time-sensitive nature of digital harms, CyberScan should consider expanding their operating hours and linking to do-it-yourself content reporting/removal resources to ensure that complainants can access immediate technological support.

EMOTIONAL SUPPORT & INFORMATION

Emotional support is the second most common response CyberScan provides. As an agent in 2020 described, *it can be a comforting and validating experience for complainants to simply speak with someone who has knowledge of cyberbullying and nonconsensual distribution and can assure complainants that they are not alone and are not at fault for having been victimized:*

> "what I hear from a lot of complainants is that it was nice just to have someone to actually talk to, and that made a big difference. And just to hear that it's not their fault. Because sometimes they are so upset when they are talking to you, and so when we tell them you know 'It's not your fault, we get calls like this all the time', a lot of feedback I always hear is 'It was so nice to just feel like I wasn't judged, I just felt so stupid that I allowed this to happen, and just knowing that someone…'. And I tell them, 'Well, this is why this unit was actually created, because this has caused so many problems for people'" (CS5).

As this agent described, it can be a powerful step in healing to have someone listen to your struggle without judgement and ensure you that you are not alone in this experience. CyberScan agents feel that their experience working in the unit makes them well positioned to comfort complainants as they can "provide understanding" of the types of harms being experienced and provide information on the supports that have been helpful for other victims (CS5). While in many cases agents provide emotional support in combination with the technological supports described above, agents also explained that in some cases emotional support is the sole support requested. As a 2020 agent described, complainants are sometimes dealing with online public shaming that is already widespread and, although little can be done to mitigate the spread, CyberScan can still provide emotional support: "[sometimes the complainant] is devastated you know, but later they will thank me and say, 'even talking to someone who knows what it's like and has that experience helped a lot'" (CS5). For complainants requiring additional emotional support, CyberScan agents also provide information on counselling and mental health supports in the community. As a 2016 agent explained, in several cases CyberScan has helped parents to find additional mental health support services for a child experiencing digital harms: "there are a lot of parents in the province that […] don't know how to use a computer, so they don't even know who to call. If they ask for information for further supports, we will take whatever time is necessary do the research we need to do to provide them with the information they request" (CS2).

While it is a positive finding that CyberScan provides needed emotional support to complainants, there are also several ways in which this support could be improved and made more accessible to all complainants. As an agent in 2016 described, it can sometimes be challenging for CyberScan staff to deal with the range of intense emotions that complainants might be dealing with when they contact CyberScan:

> "a lot of times […] emotions were very high when you get those types of phone calls. […] I would just try to listen to that person and let them know that there's somebody on the other end that would do whatever they can to help. And if there's something that we couldn't do, then to maybe give them other resources, tools they could use… but generally it was important to be there and listen and try to calm that person down and obviously help them the best way that we could. […] you're dealing with people with mental health problems at times and then obviously the people that are very much in crisis" (CS1).

As CyberScan staff are sometimes tasked with responding to people who are in serious emotional distress or crisis at the time of their call, CyberScan agents should receive training in best practices for supporting those in distress/crisis (See recommendation above: Training & professional background)*. As CyberScan deals with many cases involving aspects of sexual violence or domestic violence, agents should also receive training in best practices for supporting these victims* (See recommendation above: Training & professional background*).* Sexual violence support training is important to ensure, for example, that CyberScan agents do not engage in the kind of victim blaming and shaming that some victims of nonconsensual intimate image distribution have experienced when reporting to police (Henry et al., 2018) and that is often present in educational responses to youth (See: Education regarding nonconsensual intimate image distribution).

CyberScan's ability to emotionally support complainants is also limited by their hours of operation. While agents described some callers as being in distress/crisis and in need of immediate emotional support, the CyberScan phoneline is only open to take calls on weekdays during normal business hours. As one interviewee in 2016 explained, these limited hours of operation often make it difficult to connect with clients in need of support:

> "generally [complainants] are at work or school from 8:30 to 4:30, so I changed my hours to 8 to 4 and I kind of stay in the office through lunch hours so that I can be more accessible […]. And then obviously you want to try to hit people first thing in the morning so getting that phone call to them at 8 o'clock as opposed to 8:30 when they already left for work or school. I provide people my cellphone number so that they can access me at home if they didn't want to contact me while they're at work or if they don't get home until 5 or so then I say 'Call me at home'" (CS1).

This interviewee described making personal sacrifices to work during lunch and after hours in an attempt to reach complainants that are often not available to engage in personal or emotional phone calls while they are at work or school. This flexibility and dedication on the part of an employee is not able to, and should not be expected to, address the larger issue that complainants are not easily supported by a helpline that is only open during regular business hours. *Therefore, CyberScan should consider offering additional hours of operation (as suggested in the subsection* *above as well) and should make available a list of support services for both adults and youth that are more readily available.* There is currently a link to Kids Help Phone (who can provide emotional support for young people) on the side of the CyberScan website, but there is no information provided on what this service is or how it relates to the services available or not available through CyberScan. There is also a link to 211 on the CyberScan website, which might be used to find support services for adults, but again no information is given explaining why this link is included. Additional supports should be explained and made easily accessible to those who are in distress/crisis and are unable to immediately reach CyberScan. *In addition to linking to and explaining resources for victims looking for support outside of regular business hours, CyberScan's website should also link to resources that help bystanders learn how to best support a victim in their life.* For example, MediaSmarts provides both reassuring resources for youth victims and comprehensive resources for parents/caregivers/teachers or other bystanders on the best approaches for supporting youth victims of cyberbullying or nonconsensual distribution.

Although CyberScan was designed primarily with the intention to act as a support for youth, agents report that young people very rarely contact the unit themselves. An agent in 2020 estimated that only about 1% of calls are from those under the age of 18. Another agent explained, "kids don't call us themselves, […] it is all teachers, principals, parents or a neighbour calling, guidance councillors, it's very, very rarely a youth" (CS5). While young people may reach out to an adult in their lives that then seeks support from CyberScan, those who do not have an adult they feel comfortable reaching out to or who are not yet ready to disclose to an adult in their lives do not seem to currently be served by CyberScan. Therefore, CyberScan should consider making updates that make their support services more accessible to young people. For example, *several CyberScan staff pointed out that it may be a problem that CyberScan can only be contacted by phone, as it is well known that young people are increasingly uncomfortable making initial contact through phone calls.* Similar support lines internationally tend to provide multiple options for contact. For instance, Childline in the UK[36] provides options for support via online chat, email, or phone and the UK's Revenge Porn Helpline[37] offers options for support via Facebook Messenger, email, phone, or anonymous form. *Another limitation to supporting youth is that those under the age of 18 can only speak to CyberScan with the permission of their parent/guardian.* This policy may be limiting in many cases. For instance, youth who have their intimate images shared without consent are often concerned about telling their parents/guardians or other adults in their lives due to fears of being blamed or shamed for having consensually shared intimate images or for having been involved in a sexual situation in which images were captured without consent (Dodge & Lockhart, 2021). In such cases, youth may be looking for information about how to tell an adult in their life or information about how to report content without telling a parent/guardian that they know will judge or punish them. In such scenarios, CyberScan's service would not be accessible to them. CyberScan would also not be accessible to youth who do not have a trusting relationship with their caregivers or to youth who know that their caregivers hold discriminatory beliefs. For example, a youth who is being bullied over social media for being gay will likely not seek help if they are required to first explain the situation to their homophobic parent/guardian to get permission. Therefore, *consideration should be given to changing the policy that requires youth to get parental/guardian permission to speak with CyberScan.* At the least, CyberScan's materials should be clarified to explain that permission is required and to provide alternative supports for youth who

[36] https://www.childline.org.uk/get-support/1-2-1-counsellor-chat/

[37] https://revengepornhelpline.org.uk/how-can-we-help/how-to-get-in-touch/

are not willing or able to get such permission. For instance, the handout "Here to Help: CyberScan" states: "Anyone can contact CyberScan. This includes young people who feel they are being cyberbullied or are the victim of unwanted sharing of intimate images, their parents, teachers, principals, police, or other members of the public".[38] This handout should clarify that young people can only call with parental/guardian permission and should provide the information for alternative resources for those who do not feel comfortable disclosing to a parent/guardian.

One of the restorative approaches experts interviewed for this report asserted that there are several ways CyberScan's emotional supports could be improved by engaging restorative principles. This expert explained that, while the kind of support CyberScan currently offers is certainly *part* of what is needed to build a restorative and human-centred response to digital harm, CyberScan's response could better engage those in a victim's life as victims often experience negative consequences as a result of people in their lives acting distant or judgemental toward them in the aftermath of harm: "[Many victims of crime] will tell you that the actual fear and consequence they have following a crime is not always to do with the individual who hurt them but the ways in which they feel shunned or disintegrated [from their community]. They need to be reintegrated to their relationships with others who are afraid to ask what happened to them, or are afraid it might happen to them too, or shame them in order to keep themselves feeling like 'It couldn't be me'" (RA2). *Considering these impacts on relationships, this expert suggests that CyberScan could offer options such as meeting with family members, coworkers, schools or neighbours to help them understand the harm a victim has experienced and to help them learn how to better acknowledge this harm and support the victim rather than pushing them away.* They elaborated saying,

> "You could see CyberScan taking advantage of [Nova Scotia's] restorative justice agencies located in communities in the province [to create] more robust capacity to engage with victims and meet their needs […]. If you did have a victim who said, 'Not only do I want the [intimate] image down, but now everyone at my workplace, or church, or all my neighbours think these [negative things about] me' - there might be ways [to connect with those people to help them understand that] this person has been struggling and been harmed and that they might be able to help. There's a whole bunch of ways you could think about how to take a relational, restorative approach to those kinds of harms" (RA2).

This approach aligns well with research that has found that one of the most harmful aspects of nonconsensual intimate image distribution is often the feeling of shame or judgement this act can create between a victim and their close relations or community (Dodge, 2021; McGlynn et al., 2017). As Hamilton (2018) asserts, it is important to educate those in a victim's life about how best to provide support and avoid victim blaming and shaming beliefs. One of the restorative approaches experts also suggested that more robust supports could include finding ways to connect victims with others who have had similar experiences (RA2). They stress that *a restorative response does not have to look like organizing restorative justice circles, rather it could look like a variety of supports and services that are geared around understanding issues relationally and looking at holistic responses that consider context, causes and circumstances* (RA2).

[38] Here to help: CyberScan unit (PDF), p.2.

Recommendation #15: CyberScan's website should link to (and provide detailed information about) support lines that are open 24/7, reassuring online resources for victims, and resources that help bystanders learn how to best support a victim in their life.

Recommendation #16: CyberScan should offer a variety of options for making contact with the unit (e.g. email, text, online chat).

Recommendation #17: CyberScan should consider allowing young people to gain support from the unit without requiring parent/guardian permission. If this is not possible, CyberScan materials should clarify that this permission is required and provide alternative support options for youth who are not willing or able to get such permission.

Recommendation #18: CyberScan should consider partnering with restorative approaches initiatives to provide broader options for healing individuals and relationships impacted by digital harms.

WARNING/EDUCATING RESPONDENTS

In approximately 2% of cases[39]*, CyberScan staff contact respondents to ask them to remove harmful content and/or to stop further bullying. This is done through some combination of explaining the harm they are causing and describing the potential legal impacts of their actions. Although this approach can be useful, it is much less common than the responses above because complainants rarely wish to have respondents contacted*. As a 2020 CyberScan agent described:

> "Sometimes the complainant does not want the respondent contacted for fear that it could actually escalate the situation and make it worse… or the reasons are like 'Oh you know they are going through a hard time so I don't want you trying to contact them'. But in [a small portion] of our cases we have reached out to the respondent to kind of say 'You know this isn't acceptable, stop this behaviour' or to try to negotiate […] with them […and say] 'This is unacceptable, the victim may take you to court'" (CS7).

One CyberScan agent described how, in an attempt to avoid escalating the issue, some complainants use the information provided by CyberScan to contact the respondent themselves without involving CyberScan agents directly:

> "I've had some cases with adults where just sending them the information on CyberScan, they felt that was helpful because then they sent it to the person that was bothering them saying 'Look if this continues, I've already contacted CyberScan and they will be in touch if… like I don't want this to continue'. And that's been enough sometimes, even to send

[39] This is a rough estimate based on somewhat informal records kept by CyberScan staff from July 5th, 2018 to November 5th, 2020.

> them the link and them to see that there is actually an organization that helps with this kind of stuff' (CS5).

In some cases, it seems that simply warning or educating the respondent that the perpetration of digital harms can have consequences is enough to end the cyberbullying or the nonconsensual distribution of intimate images. However, agents explained that it is sometimes difficult to engage adult respondents, as opposed to youth who can be engaged through the school system, because adults may simply refuse to speak with CyberScan agents: "the adult cases, they were the trickier ones for sure, because lots of them […] didn't want to meet with us. So we might have to then draft a letter to send to them in the mail just saying who we are, explaining the legislation a bit, and asking them to stop that way" (CS4). Therefore, this response is used less frequently due to both the lack of interest in this option on the part of many complainants and the inability to compel respondents to engage with the unit. However, *in the rare cases in which this approach is used, CyberScan agents described simply speaking with respondents as often capable of resolving issues.*

CyberScan is faced with many challenges when contacting respondents. As discussed above (See: History of CyberScan), some CyberScan agents working under the original *Cyber-safety Act* (2013) may have used warnings of potential legal consequences in a manner that unduly limited "legitimate *Charter*-protected speech" (Fraser, 2017). *Although continued attention will need to be paid to striking the right balance between providing warnings/education about potential legal consequences and respecting the rights and interests of respondents, the limited legal tools available under the current legislative framework makes undue limits on respondents less likely (See:* Use of civil court orders*). Nonetheless, it is important to consider the tone and messaging that CyberScan uses when contacting respondents.* For example, CyberScan must decide how to balance warnings/education regarding potential legal repercussions with education about the harms that respondents are causing. The restorative approaches experts interviewed for this report stressed that engagement with respondents should focus on expressing that their behaviour is harming others rather than focusing on the use of law as a scare tactic. That is, potential legal consequences should be framed as a last resort rather than as *the* reason not to commit harm.

It is not entirely clear from the interviews how CyberScan agents balance legal warnings versus discussion of relational harms. One agent in 2016 seemed to describe focusing more on education about the harm caused than on the threat of legal actions: "[the goal of contacting the respondent was] to end [the cyberbullying] in a way that had the respondent taking responsibility for the damage they may have caused or at least an understanding or awareness of what they've done and how it impacted others" (CS3). While this agent stressed the need for respondents to understand the impact of their actions on others, the other agents interviewed in 2016 seemed to focus much more narrowly on stopping conduct through warnings about potential legal consequences. As a 2016 agent explained:

> "We would seek out the respondent, the cyberbully, and the goal would be try to meet with them and explain the legislation, explain the potential consequences of the legislation, but ask if they'd agree to an informal agreement which would typically be to remove the cyberbullying content, not to engage with the victim […] of the cyber bullying in the future, or whatever we deem appropriate for the situation we're dealing with. And if that

> individual agrees to those terms, then we would document everything within our database and that would be the end of the file" (CS2).

This approach demonstrates a focus on legal warnings and pressure to agree to a set of pre-determined actions and limitations under threat of legal action. This response seems to disregard any meaningful discussion of relational harms or negotiation about appropriate next steps.

Although the approach taken by agents in 2020 is also somewhat unclear from interview responses, it does seem that the tone of engagement has moved more toward education and awareness of relational harms. This change in tone is likely partially due to the changing legal tools available to agents that have limited their ability to use threats of legal action. An agent in 2020 described sometimes contacting respondents without mentioning legal consequences at all: "I had a case the other day where he was just receiving a number of different unwanted messages and stuff and so I called the respondent and I said 'You know I've just received a complaint from this guy and he doesn't want you emailing him anymore', so that is kind of a little bit of a resolution by just kind of bridging that gap between both people" (CS5). However, in cases of nonconsensual intimate image distribution, which is a clearly criminalizable act, a CyberScan agent in 2020 described focusing on legal warnings as their main tactic: "Sometimes [the complainant] will say 'Could you talk to him and let him know that this could be a criminal offence even though I don't want to go that route?' So I love that it's a criminal code offence because it makes my job a lot easier, because that is the threat I can kind of use I guess… to call the respondent and say 'She is asking you to take this image down, this could be a criminal offence'" (CS5). Explaining the law to a respondent and asking them to remove nonconsensually shared intimate images can act as an expedient way to stop the harm of this act; However, CyberScan agents should consider, even in these clearly criminalizable cases, how they want to balance education about the harms being caused with warnings of legal implications.

As the restorative approaches experts interviewed for this report explained, *there are several ways to consider a more restorative approach to engaging with respondents.* As one expert explained, "when they call the perpetrator […] it is an opportunity for education and there are a variety of ways you could be inclusive, participatory, forward focused, comprehensive and holistic. All those principles could still show up […] if they want to be restorative. But you couldn't call it restorative if they are just calling somebody and saying 'Got to take the image down, it's against the law'" (RA1). This expert further explained,

> "A focus on the law […] is what brings people together if you are taking a restorative approach, […] but that's step two to talk about the law. Let's focus on talking about the harm that you caused rather than the law that you broke. […] [So rather than just saying] 'Here is the law you are breaking, you should think about this', you are saying 'Hey, what's going on? Do you want to enter into a process where we figure this out?' […] There are different questions you could ask, different things that you could say, that are meant to prompt the person to be thinking differently"[40] (RA1).

[40] Ted Wachtel (2016)explains that "informal" ways of engaging restoratively (e.g. asking questions that engage relational thinking) have a "cumulative impact and creates what might be described as a restorative milieu—an environment that consistently fosters awareness, empathy and responsibility in a way that is likely to prove far more effective in achieving social discipline than our current reliance on punishment and sanctions".

In working toward taking a more restorative approach, agents should also consider what supports respondents might need to deal with the issues or circumstances that led to their perpetration. Taking a relational approach, supports should be human-centred and not just victim-centred so as to recognize and address "the experiences, needs, and perspectives" of all the parties involved (Llewellyn et al., 2014). *CyberScan should consider the ways perpetrators of harm could be better supported to acknowledge the harm they have caused, to change their behaviour, to help heal harm caused, and/or to receive support for their own needs.* Addressing the needs of all parties is especially important in the context of bullying and cyberbullying as the literature finds that perpetrators of bullying are often victims of bullying as well (Beran et al., 2015). As the director of education for MediaSmarts explains, "it's not at all uncommon, for example, for someone to be the aggressor in one relationship and the target in another, or for victims to try to retaliate against their harassers. […] In classroom bullying, for instance, high-status youth often keep their bullying 'under the radar' until the target retaliates – at which point she is usually the one punished. In a painful irony, cyber-bullies often use mechanisms designed to fight bullying as a tool for bullying by threatening to 'report' their targets".[41] Therefore, the "victim" and "perpetrator" roles may not always be so clear or consistent. As one CyberScan agent described, it can also be the case that a bully begins to be bullied for their actions in a way that creates more harm rather than creating accountability: "Public shaming is a big thing on the internet, all of a sudden the whole small town is talking about this kid that did this [bullying], and its adults actually publicly shaming this youth" (CS5). This agent explains that, in youth cases especially, the family of the respondent is also sometimes cyberbullied for being "bad parents" in the aftermath of harm (CS5). These examples demonstrate that a simple victim/perpetrator dichotomy does not always exist in cases of cyberbullying[42] and that addressing the particular issues in a case will often require attention to the needs of all parties and impacted relationships (*Cyberbullying Hurts: Respect for Rights in the Digital Age*, 2012; Fairbairn et al., 2013). *It is also necessary for CyberScan to learn from the actions of individual respondents to determine what broader educational and systems-level changes are needed to prevent or better address future acts of harm* (e.g. a lack of knowledge about the harms of nonconsensual intimate image distribution in a particular age group or community could signal the need for further public education about this act that is targeted at that particular group).

> *Recommendation #19: Approaches to engaging respondents should be consistently assessed to ensure they are not unduly limiting respondents' legitimate expression.*
>
> *Recommendation #20: CyberScan agents should consider taking a more restorative approach to engaging with respondents and should carefully assess how they are balancing discussions of relational harms with information about potential legal consequences.*

[41] https://mediasmarts.ca/blog/shades-grey-rethinking-cyberbullying-interventions

[42] The victim/perpetrator roles can also be more complicated in cases of nonconsensual intimate image distribution in which images are shared without consent because the person "had received those images against their will, making them both victims and perpetrators" (Naezer & Oosterhout, 2021, p. 9).

> *Recommendation #21: CyberScan should consider the ways perpetrators of harm could be better supported to acknowledge the harm they have caused, to change their behaviour, to help heal harm caused, and/or to receive support for their own needs.*

RESPONSES TO YOUTH CASES

This section discusses the specific responses that CyberScan provides in youth cases. The first subsection discusses CyberScan's school-based responses to individual youth complainants and respondents involved in cases of cyberbullying or nonconsensual intimate image distribution. The second subsection discusses the educational presentations for youth that CyberScan often provides as a preventative measure and/or in the aftermath of an act of cyberbullying or nonconsensual distribution. The third subsection discusses CyberScan's approach to education on the topic of nonconsensual intimate image distribution. The final subsection discusses specific concerns that arise in responding to youth (under the age of 18) cases of consensual and nonconsensual intimate image distribution due to the problematic labelling of these acts as "child pornography".

SCHOOL-BASED RESPONSES TO YOUTH COMPLAINANTS & RESPONDENTS

Prior to 2016, CyberScan agents regularly worked closely with school principals to respond to individual cases of digital harm among youth by meeting with the various parties involved. However, agents interviewed in 2020 explained that they are now most often contacted by school principals after a case has already been dealt with by the school, and the principal simply requests that CyberScan provide a "cyber safety" presentation. Agents in 2020 were unsure why exactly CyberScan has largely moved away from the more involved school-based responses described in 2016: "We could [meet with the parties involved], but we don't do it a whole lot, surprisingly. I've done it a few times in the schools, where actually the teacher and myself and the two parents and both youth all sit down and kind of talk about what happened and how we are going to move forward and that kind of thing, but typically we don't do a whole lot of that" (CS5). It seems that one reason for this change in approach is that schools currently view CyberScan largely as a resource for educational presentations in the aftermath of cases: "Typically if the school calls and there is an issue between two students […] the school may have already dealt with it through a suspension or something, but then like they are saying 'Can you come to the class and speak to the whole class about some of the detrimental effects of cyberbullying or of passing an intimate image without consent?'" (CS5). *Because it is unclear why exactly the relationship between CyberScan and school has changed, CyberScan and schools should work together to explore whether the current relationship uses CyberScan to its full potential or whether other supports and responses could be offered.*

As this subsection analyzes CyberScan's school-based responses to individual youth complainants and respondents, it draws primarily from interviews with agents who worked more closely with schools prior to 2016. Agents interviewed in 2016 reported that their assistance with school-based responses usually involved the following steps: CyberScan is contacted by a school official (usually the school principal) regarding a case of cyberbullying or nonconsensual intimate image distribution; CyberScan speaks with the complainant and their caregiver(s) to gather evidence about the incident; along with the principal, and potentially other parties (e.g. school councillor), CyberScan meets with the complainant and their caregiver(s) to provide education regarding cyber safety; along with the principal, and potentially other parties (e.g. school resource officer), CyberScan meets with the respondent and their caregiver(s) to have them remove any remaining harmful digital content, create an informal agreement to stop the behaviour, and provide them with education about the relevant civil and/or criminal laws that could apply if they continue this behaviour (CS1). Prior to 2016, CyberScan agents were regularly traveling to schools throughout the province to hold these hour-long school-based meetings with complainants and respondents (CS2). Agents in 2016 described this approach as quick and effective: "You can have back-to-back meetings and resolve the issue as quickly as possible within a day or two" (CS2). *While expediency is helpful in terms of the initial response, immediate interventions should be followed by deeper and ongoing responses that address the core issues revealed by a case*. Both restorative approaches experts stressed that responses to youth cases should not simply be aimed at getting an agreement from the respondent that the harmful behaviour will stop, but rather should aim to understand and address the "contexts, causes, and circumstances" behind the harmful act and to "build a more robust approach to safety and wellbeing in schools" (RA2). As CyberScan agents drop into a school for a few hours or days and then leave, they should work with schools and caregivers to cocreate plans for providing ongoing and holistic responses after they have left.

From a restorative perspective, responses to individual cases of harm should act as a catalyst to consider what relational and systems-level changes are needed to address the broader issues that are revealed by individual cases. Despite being envisioned early on as a resource for providing a robust restorative approach in schools, CyberScan does not currently work with schools to consider ongoing interventions in the aftermath of harm (See: Taking a restorative approach?). Rather, CyberScan's standard intervention currently entails providing a short "cyber safety" presentation, the limits of which are discussed in more detail in the subsection below. *One of the restorative approaches experts explained that the early vision for CyberScan was that agents would help schools respond to individual cases to immediately stop the harmful behaviour, but would then take the time to say "Now let's talk about what's going on here more broadly" (RA1).* For example, an individual case of homophobic cyberbullying would be a catalyst to ask: What about the school and community environment is sending the message that homophobia is acceptable? And what changes would need to occur at the level of interpersonal relationships, school policy/practice, and community to address this? Helping to coordinate a robust approach, a CyberScan agent might work in collaboration with school staff, community organizations, and students to craft a plan that, in the example of homophobic bullying, might include supporting the creation of a gay-straight alliance with the help of the Youth Project, adding discussions of LGBTQ+ rights and historic figures into various class curriculums, educating teachers and school staff on how to ensure they are modelling the use of inclusive language and are addressing instances of homophobic bullying in the classroom, and ensuring that school policies and practices support equality and inclusion. An individual case reveals that "a person has a particular view of what's okay or lacks the understanding of how this could impact a person", and that information can be used to "inform what the guidance counsellor is talking to kids about, what kinds of conversations teachers are having day-to-day in a classroom, and it ought to inform a whole bunch of other things that we do in terms of the school system" (RA1). One of the restorative approaches experts explained that CyberScan should look at broader "systems, policy, practice, or messaging that needs to change" within a school because, “if they aren’t feeding [what they are learning from individual cases] back up to the system and doing things different in the system, then what we have are […] responses that make things marginally better for [individual students] but then we just have a new crop of students come in the next year and the whole cycle starts again” (RA1).

In terms of ensuring ongoing impacts from CyberScan’s interventions in youth cases, it is also necessary for CyberScan agents to reflect on how they balance legal warnings versus helping the respondent understand the harms and relational impacts of their actions. As discussed above (See: Warning / educating respondents), it is important to help all wrongdoers, but especially youth, to realize the relational impacts of their actions on others rather than primarily using scare tactics about how potential legal consequences could negatively impact *them*. As a restorative approaches expert explained, legal warnings have “a short term impact and, in the school system especially, we should be very worried about the long term implications and having people understand the impacts of this behaviour in a way that isn’t just talking about the legality” (RA1). A 2016 agent described CyberScan’s approach to meeting with youth respondents in the following way: “The first thing we would do is explain the *Cyber Safety Act*, […] we’d go through the law and what the law means, we’d explain that we’d like to resolve everything informally in the first instance, but we’d explain what the legal consequences were if it continues. And then if it […] involved intimate images, we’d explain what the criminal law is as well and go through all that with them” (CS2). This very law-focused approach, which was described by several agents in 2016, is not the most impactful way to engage youth respondents. Youth are unlikely to refrain from harmful behaviour just because there is a law; Rather, they are more likely to change their behaviour if those close to them express their disappointment in the behaviour and help them understand the relational harms their behaviour is causing (*Cyberbullying Hurts*, 2012, p. 314; (Morrison, 2002, p. 6; Russell & Crocker, 2016). As restorative approaches experts assert, responses to youth wrongdoing should help youth understand how their actions negatively impacted “relationships in the school and wider school community”, rather than simply asserting that it is wrong because it violated the law or school rules (Morrison, 2002, p. 6; Russell & Crocker, 2016). As Wendy Craig reported to the Senate of Canada, bullying is a relationship problem that requires relationship solutions (*Cyberbullying Hurts*, 2012). *Therefore, youth respondents should be helped to understand the consequences of their behaviour in a way that develops “relational thinking” (Morrison, 2002, p. 6; Russell & Crocker, 2016) and treats legal education as a carefully communicated secondary goal.*

CyberScan should also carefully consider which people are most appropriate to bring into meetings with youth respondents. *Namely, bringing a school resource officer into these meetings, which agents in 2016 described as a regular occurrence, could move the meeting toward a less successful “scare tactic” or “law and order” approach.* As one of the restorative approaches experts commented,

> “[I] worry about automatically bringing […] the school resource officer in. [What I would say to principals] is ‘Stop bringing your resource officer in to scare those kids straight’. If you want to bring those resource officers in it could be to say ‘Hey, […] this is why I’m worried about you’ or ‘This is the sort of ripple effects that you are having on the families and the community’, to help a young person understand what you see as a police officer as the impact of their behaviour. But not focusing in on […] ‘Right now I could arrest you!

> Right now you're getting a caution, but do it again and I'm going to arrest you!' […] [When deciding whether to bring] that resource officer in, [don't do it] unless they are bringing them in to talk to that child in a way that will help them expand their understanding of the impact, otherwise you are just doing a law and order approach" (RA1).

The inclusion of school resource officers should also be questioned due to growing uncertainty regarding the appropriateness of using police as a resource in schools, especially considering evidence that their presence has particularly negative impacts on marginalized youth (Boyd, 2020; Vitale, 2017). As CyberScan agents are able to respond informally in almost all instances of digital harm, a representative of the criminal justice system may be an unnecessary presence in these meetings, especially as one of CyberScan's core roles is to provide any legal insight that may be needed. Instead of including police officers, attention could be given to who could be helpful in addressing the specific case at hand. For example, in a case involving nonconsensual intimate image distribution it could be useful to have a sex educator present who can speak to the importance of sexual consent.

Finally, CyberScan should also carefully consider the messages they communicate to complainants in their school-based responses. CyberScan agents in 2016 described providing youth complainants with "cyber safety tips" in the aftermath of harm. These tips included telling complainants to use privacy settings to limit who can see their social media profiles and to limit their social media contacts to include only those they know in real life (CS4). In most cases reported to CyberScan, the perpetrator of harm is someone known to the complainant and, therefore, such "cyber safety" precautions taken by the complainant would not have prevented the harm and may not feel like relevant support in the aftermath of bullying involving their peers, ex-partners, or others that they interact with in their integrated online/offline lives*. Some approaches to providing "cyber safety" tips could also make the complainant feel as if they are being judged for the harm they experienced.* An agent in 2016 described that agents would sometimes review a youth complainant's social media profile and provide "cyber safety" advice based on what they saw: "We would discuss stuff that wasn't specific to the investigation but that I was able to view online as I was investigating, you know posting provocative photographs that are open to the public that anyone can take and post anywhere else, and just give them some safety tips about that" (CS4). Complainants might find it an invasive or shaming experience to have their personal social media accounts examined and critiqued by a government enforcement agent in this way. While it can be useful to help youth think critically about some of the things they might want to consider when crafting their online presence, agents should avoid making moral judgements or giving prescriptive advice about a young person's self-expression. *In cases involving digital forms of sexual violence, "cyber safety" tips could especially come across as blaming or shaming.* For instance, in the aftermath of nonconsensual intimate image distribution, it can be harmful to provide responses that assert the victim is responsible if they consensually shared intimate images that were later shared without their consent (See: Education regarding nonconsensual intimate image distribution). Therefore, *CyberScan agents must research best practices in terms of education and support for complainants to ensure their messaging is appropriate, relevant, and avoids victim blaming or shaming.* Useful resources for providing appropriate supports include, for instance, Project Shift's guide for supporting girls who are impacted by digital harm[43]. This guide includes practical tips for supporting girls, such as ensuring that responses to digital harm do not make

[43] https://mediasmarts.ca/sites/mediasmarts/files/guides/ywca-guide-for-trusted-adults.pdf

"girls feel scared and helpless […] by exaggerating the risks of being online […] and instead make sure they feel that they have the tools to deal with whatever negative experiences they face and that they have trusted adults they can count on if things go wrong"[44].

> *Recommendation #22: CyberScan and schools should work together to explore the most meaningful and useful ways they could collaborate moving forward.*
>
> *Recommendation #23: CyberScan should consider taking a more restorative approach to youth cases that provides holistic/ongoing responses, carefully considers what parties are most appropriate to including in discussions with youth, focuses on the relational impacts of wrongdoing, and uses individual cases of harm as a catalyst to consider what policy, relational, and systems-level changes are needed to address the deeper issues revealed by a case.*
>
> *Recommendation #24: CyberScan agents must research best practices for supporting and educating youth impacted by cyberbullying or nonconsensual intimate image distribution to ensure their messaging is appropriate, relevant, and avoids victim blaming or shaming.*

EDUCATIONAL PRESENTATIONS

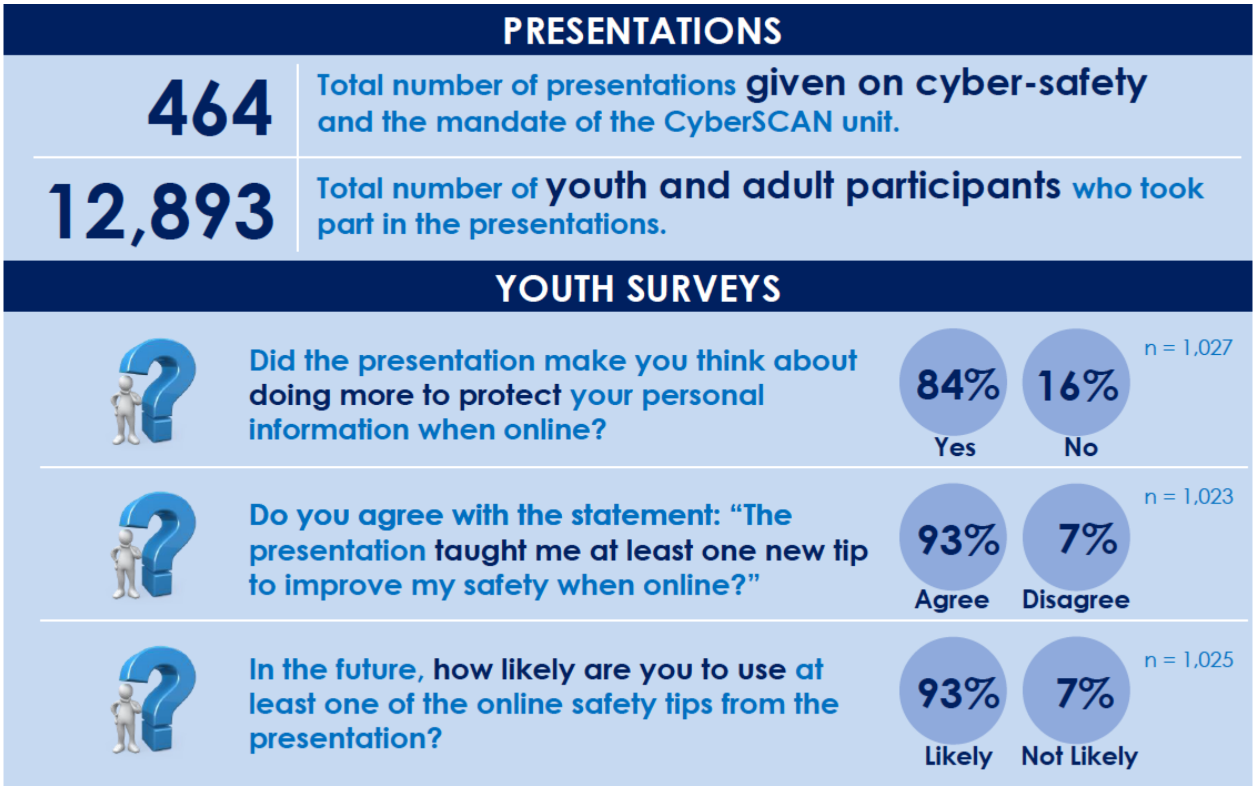
CyberScan's mandate includes providing educational presentations on cyberbullying and nonconsensual intimate image distribution to Nova Scotians. This mandate has primarily been responded to in the form of "cyber safety" presentations for youth.[45] A significant amount of CyberScan agents' time is spent providing these presentations. As an agent in 2020 explained, "there is only two of us doing this right now, it works out to about 20 presentations a month […] so it's still a big part of our job, and we get lots of requests from schools […] to do them" (CS5). Between 2013 and 2017 agents provided over 900 cyber safety presentations[46] and between July 5th, 2018 and July 5th, 2020 agents provided 464 presentations (See infographic below). A 2016 agent explained that these presentations are aimed primarily at meeting CyberScan's prevention goals by educating "the province about the law and educating Nova Scotians about the harm of cyberbullying and that it's illegal to do it" (CS2). *It is necessary to closely analyze whether the educational approach taken in these presentations is appropriate to the goal of preventing cyberbullying and nonconsensual intimate image distribution.*

[44] https://mediasmarts.ca/sites/mediasmarts/files/guides/ywca-guide-for-trusted-adults.pdf, p.23-24.

[45] Although CyberScan also provides some presentations to adults (generally government staff or community service providers) on the *mandate* of the CyberScan unit, this subsection focuses specifically on the cyber safety presentations provided to youth. This focus is taken both because presentations for youth are more common and because suggestions for improved communications about CyberScan's mandate are already provided in the section above titled Communicating CyberScan's role.

[46] Nova Scotia, Legislative Assembly, *Hansard*, 63rd Leg, 1st Sess, No 27 (12 October 2017) at 1166.

CyberScan's cyber safety presentations for youth are typically provided in schools and are delivered either to individual classes or in a school assembly. Presentations are often requested with the general goal of prevention: "we'll just get a call where a principal says, 'We have all new grade 6 students starting this year, do you mind meeting with all the grade 6 students just to get them off on a good foot and talk about cyber safety?'" (CS5). At other times, presentations are requested in the aftermath of a particular act of digital harm or to try to address ongoing acts of harm (CS2). Agents generally expressed feeling that these cyber safety presentations are effective. They provided examples of positive impacts such as the takedown of an anonymous rumour account following a presentation in a high school assembly (CS2) and an elementary school student reporting an incident of cyberbullying because they learned through a presentation that it was against the law (CS5). Between July 5th, 2018 and July 5th, 2020, agents also measured success through having youth complete surveys following CyberScan presentations. The image below is a portion of an infographic made by CyberScan to display the results of these surveys. As shown in this infographic, the majority of youth surveyed by CyberScan reported that they learned tips to improve their online safety. *While the results of this survey imply that CyberScan's educational approach is successful, it is necessary to assess whether the learning outcomes being measured are appropriate for preventing cyberbullying and nonconsensual intimate image distribution.*



PRESENTATIONS

464	Total number of presentations **given on cyber-safety** and the mandate of the CyberSCAN unit.
12,893	Total number of **youth and adult participants** who took part in the presentations.

YOUTH SURVEYS

Did the presentation make you think about **doing more to protect** your personal information when online?	84% Yes	16% No	n = 1,027
Do you agree with the statement: "The presentation **taught me at least one new tip** to improve my safety when online?"	93% Agree	7% Disagree	n = 1,023
In the future, **how likely are you to use** at least one of the online safety tips from the presentation?	93% Likely	7% Not Likely	n = 1,025

Based on the survey questions asked (See infographic), as well as interviews with CyberScan agents and a review of the PowerPoint slides used for their cyber safety presentations, *it seems that CyberScan's presentations are aimed primarily at giving youth "cyber safety" tips (e.g. limit who can see your social media profile, don't accept friend requests from strangers, don't share your home address online) that are more appropriate for avoiding instances of harassment, luring, or stalking by strangers than for preventing cyberbullying or nonconsensual intimate image distribution.* While these are generally desirable tips for youth living in the digital age, there are several reasons why they do not necessarily align with the goal of preventing or responding to cyberbullying and nonconsensual intimate image distribution. For example, *the vast majority of CyberScan's cases involve a respondent and complainant that are known to each other offline, yet CyberScan's cyber safety tips seem to focus largely on addressing "stranger danger" scenarios and online privacy infringements.* A CyberScan agent in 2016 explained that their cyber safety presentations teach youth:

> "About privacy settings, […] about how easy it would be for a stranger to find out where you live with your GPS on. […] So just trying to build awareness that when you're on social media and you're in the comfort of your own home, and you have like your GPS on, everyone in the world physically can see where you are. And that was the other big topic was about not talking to strangers online. Teaching youth […] how to put your privacy settings on. How to keep yourself safe." (CS4)

A 2020 agent similarly described their presentations as helping youth to "realize how open their profiles are" and to ensure that only people they know offline can see their social media profiles: "[We tell youth to] make sure you are aware of who can see your posts and who can contact you. Accept only messages from those on your friends list and make sure only friends can see your location. Tidy up your friends list and delete those you don't actually know" (CS5). The PowerPoint presentation for youth in 2020 likewise provides safety tips that are primarily aimed at avoiding harm/privacy-infringements at the hands of strangers, such as: "Don't post personal information online (no phone number, address or school); Use only your first name or nickname; Use privacy settings; Make sure your device has a lock code"[47].

There is a clear disconnect between these cyber safety tips, which are focused on avoiding the exposure of personal information and location to strangers[48], and the kinds of cases CyberScan most often responds to (i.e. cases in which complainants and respondents are known to each other offline and bullying/harassment is often occurring both online and off [49]). As Fairbairn et al.'s (2013) study of digital sexual violence found, "because the majority of sexual violence associated with social media is perpetrated by someone known to the individual, blocking programs and privacy controls are less likely to be effective prevention mechanisms" and preventative education "should recognize that online victimization is not primarily 'stranger-danger'" (p. 6). They recommend that online safety advice should be treated as a "tip for protection, not a road to prevention" (Fairbairn et al., 2013, p. 6). Likewise, best practices in youth education for cyberbullying more generally tend to avoid the kind of cyber safety model that CyberScan currently utilizes. As the education director for MediaSmarts explains, interventions that focus on a cyber safety model, rather than addressing complicated relational dynamics and discriminatory beliefs, "are bound to fail" [50]. One of the restorative approaches experts likewise commented on the inappropriateness of the cyber safety model for addressing these relational issues saying:

[47] CyberScan PowerPoint slides for grades 4,5, & 6.

[48] At times, it even seems that a "cyber safety" focus has resulted in CyberScan's presentations veering into discussions of adult predators luring children online, which is a very different issue than those peer-to-peer cases that CyberScan was created to respond to. As an agent in 2016 described, "we talk about child luring cases, child protection, and child exploitation cases" (CS4).

[49] As a CyberScan agent described, "I mean cyberbullying usually doesn't stop at cyberbullying, so there's also going to be some bullying going on at school too, you know" (CS2).

[50] https://mediasmarts.ca/blog/shades-grey-rethinking-cyberbullying-interventions

"[Acts of cyberbullying and nonconsensual distribution] are almost always tied up in complex emotional reactions, responses, and pressures around sexuality, identity, relationships, and hurt. So it's just tone deaf to turn up and think that privacy or technology is the problem, it just gets the problem wrong. And then [youth] really don't listen to you if you don't have the problem right" (RA2). *The cyber safety model is also problematic because it puts the onus squarely on potential victims to avoid being harmed and does little to address why youth harm each other and what would need to change about their behaviours, and the contexts and circumstances around them, to make this less likely.* Research has found that when "children and youth are primarily educated about digital technologies through an 'online safety model' that focuses on protecting themselves and avoiding 'risky' activities", they may learn to responsibilize victims for the harms they experience rather than learning what ethical behaviour looks like (Mishna et al., 2020, p. 419; Naezer & Oosterhout, 2021). *Education that focuses primarily on discussions of the victim's role in avoiding harm can be counterproductive by invisibilizing the actions of perpetrators and implying that the cultures that support bullying are natural and unchangeable (Mishna et al., 2020).*

The current cyber safety approach does not seem to address the kinds of harmful interpersonal conflict, discriminatory bullying, or digital sexual violence that CyberScan was created to respond to. Demonstrating the incongruence between "cyber safety" tips and the core issues CyberScan was created to address, the harm committed in the Rehtaeh Parsons case[51] (i.e. the catalyst for creating the CyberScan unit) would likely not have been prevented or lessened by the current approach to cyber safety education. Nothing Rehtaeh could have done in terms of securing her privacy settings or avoiding strangers online would have addressed the sexist bullying and victim blaming/shaming that she experienced from her peers online and off. To alleviate the harms in cases such as this, education would need to address sexist and victim blaming/shaming beliefs and teach students how to support victims of sexual violence and nonconsensual intimate image distribution. As Rehtaeh's father put it in a recent interview, "a lot of people think that Rehtaeh died because she was cyberbullied — and it played a part of that — but a bigger part of her entire story really is a story about victim-blaming and misogyny" (Cooke, 2021). Likewise, Segal's review of the handling of the Rehtaeh Parsons' case states, "I wholeheartedly agree that the true solution to the problem lies in the evolution of societal norms related to sexual assault specifically, and gender equality more broadly" (Segal, 121). *CyberScan's current cyber safety model of education does not seem to be aimed at challenging the culture beliefs that fuel the harms of sexist bullying, victim blaming/shaming, or other discriminatory beliefs that are often present in the most harmful experiences of cyberbullying and nonconsensual intimate image distribution.* When asked whether CyberScan's presentations address discriminatory beliefs (e.g. sexism, victim blaming/shaming) or discuss healthy relationships, an agent in 2020 responded:

> "No, we don't. That would be great, and I know the schools would like something like that, but we only have like 40 minutes. We basically talk about the social and legal detrimental effects of cyberbullying and passing an intimate image, and some of the things that could result from that, and then we always talk a lot about cyber safety. But we don't [talk about healthy relationships or discrimination]. And we're not really educators either, so our […]

[51] Parsons died by suicide in the aftermath of having an intimate image of her (captured during an alleged sexual assault) nonconsensually distributed and used as fodder for sexist and victim blaming/shaming bullying and harassment by her peers.

> presentation is very specific [to cyber safety] […]. But yeah [it would be good to] even be teaching them what is a healthy relationship, or that if someone is continually asking you to do something you're uncomfortable with, like that is really not okay. And I don't know if [the schools] teach really anything like that even" (CS5).

As agents do not currently address the core issues that underly cyberbullying and nonconsensual intimate image distribution, and do not have training in education, much work is needed to make CyberScan the robust educational resource that it could be.

While CyberScan's current educational approach seems to primarily responsibilize potential targets to avoid harm through cyber safety tips, best practices in addressing cyberbullying and nonconsensual distribution (such as those described by MediaSmart[52] and by education scholars[53]) assert that education should be focused on challenging discriminatory beliefs, unequal power dynamics, and exclusion of those who are different. *Education should aim to create "a culture where bullying is not seen as the norm"[54] and should teach youth the importance of healthy/ethical relationships, consent, diversity/inclusion, and empathy*. CyberScan agents should consider working in collaboration with organizations in the province that specialize in providing education to youth on these topics. For instance, the educator for the Youth Project specializes in providing workshops on diversity/inclusion and would be well-suited to help address issues of homophobic or transphobic bullying in schools. In regard to consent and healthy relationship education, CyberScan might seek support from regional Sexual Health Centres that can provide multiweek programming that embeds conversations about nonconsensual intimate image distribution and digital relationship abuse into broader discussions of healthy relationships and consent. *Adequate resourcing to community and government organizations that provide education on these topics is needed to provide robust educational responses to the core issues that underly digital harms.*

Education will also be more successful if it speaks to the particular issues a school is dealing with, is cocreated by those in the school or community, and engages youth rather than "talking at" them. One of the restorative approaches experts suggested that, when a school requests a cyber safety presentation from CyberScan, agents could begin by discussing what particular issues the school is facing and offering more engaging and tailored options than a standard presentation:

> "Say to the school 'Look tell us what you're hearing, what are the trends here, tell us a little bit about what kids think', and then go back and look at the resources that [CyberScan] has available and […] come back to the school and say 'Here's how we could help.' […] So come back to that school with some material that is relevant to the kids, maybe we've designed some talks with the kids, we have some focus groups planned for the kids, like we could do a whole project right? […] [CyberScan could say] 'Well we don't just do presentations… I could just give you the slide deck and your guidance councillor could do this presentation if that's all you want. You don't need the CyberScan investigators to come

[52] https://mediasmarts.ca/blog/shades-grey-rethinking-cyberbullying-interventions

[53] https://www.mcgill.ca/definetheline/resources/resources-educators

[54] MediaSmarts explains that making "not bullying" the norm can be done, in part, through a process called "social norming" in which "positive behaviours are reinforced by making members of a group aware of how common they are" and how much less common harmful behaviours are than youth assume (See: https://mediasmarts.ca/blog/shades-grey-rethinking-cyberbullying-interventions).

> in […] for that. We could do so much more. […] We could go in and we could facilitate conversations, or we could meet with families, or we could come in and work differently, work restoratively, with you'" (RA1).

Education will be more successful if it is tailored to a particular student context and is provided through interactive workshops/discussions rather than through a standard presentation. Rather than providing cyber safety tips that could be passed on through a video presentation without bringing in CyberScan, class time could be spent engaging with students about their beliefs regarding the challenges that digital technology can bring to having respectful relationships, the supports they use when they are struggling, and the ways that they want the school to help support them: "[Young people] are way more experts on what actually leads to escalating tensions online and what would help keep them safe or get help than any of those people standing in front of the classroom are" (RA2). *There is a great deal of evidence that providing presentations that "talk at" young people, rather than engaging them in open discussion or change making activities, will have limited impacts and may be simply tuned out by youth*[55.] As a restorative approaches expert put it, "if you're going to spend curricular time, don't just have them come and do a little presentation, […] no one learns that way" (RA2). Rather education can help "build the capacity for people to understand their obligations to one another and impact on one another", "to gain the capacity to talk about difficult things", and to begin thinking critically about the ways they interact online (RA2). Project Shift is an example of an educational resource that provides questions to start this kind of open conversation with youth about the challenges and supports they need to deal with harms and relationships in a digital world. This resource suggests asking questions such as: "What questions do you ask yourself before you post or share something?" and "What would you do if you saw someone being harassed online?" [56].

By cocreating educational responses with school staff or community organizations, CyberScan would also be able to ensure that educational interventions build capacity for ongoing responses once CyberScan agents leave. One of the restorative approaches experts asserted that it is not the most impactful approach to have a CyberScan agent, who students have no pre-existing or ongoing relationship with, provide a single presentation to students (RA1):

> "Kids will tell you that […] having an expert come in that the kids don't know and don't have a relationship with does not have the same impact as the people they have a relationship with, so the teachers they trust, the guidance councillors they trust. So it's not that somebody can't come in and technically do a good presentation and share information… but that information lands differently for the children than if that very same information was part of a regular conversation that a teacher or other staff member is having with the kids every day […]. A restorative approach to cyberbullying […] cannot be only on the plate of the CyberScan unit, there has to be this relationship with the school system that says, 'Here is this unit, how can we leverage this relationship and this very good resource to work differently with schools to address cyberbullying?'" (RA1)

Education experts and restorative approaches experts warn against "one-time interventions", as it is much more effective and engaging to provide "programs that are planned to go on through the

[55] https://mediasmarts.ca/blog/shades-grey-rethinking-cyberbullying-interventions

[56] https://mediasmarts.ca/sites/mediasmarts/files/guides/ywca-guide-for-trusted-adults.pdf, p.25.

entire school year" that help create a day-to-day environment of care and trust in which young people are able to ask for support, have difficult conversations, and learn ethical behaviour (*Cyberbullying Hurts*, 2012, p. 82; RA1; RA2). Instead of providing a single 40-minute presentation, CyberScan could, for example, help design a series of workshops on healthy relationships on and offline to be provided by the school's guidance councillor throughout the year. Using this approach, students learn about these issues in an ongoing way and receive these messages from those in their lives that they can go to for support. Likewise, cocreating education with community organizations allows young people to be familiarized with and seek supports from those who will continue to be present in their community or school. While a CyberScan agent might present on the topic of nonconsensual intimate image distribution in Amherst and then drive back to Halifax, a similar workshop could be delivered by Cumberland County's Sexual Health Centre as part of their multi-week healthy relationship education and could end by encouraging youth in Amherst to stop by the centre if they ever need additional information or support on this topic. *When educational approaches are cocreated with school staff or community organizations they can: be tailored to the specific school environment; include ongoing workshops, focus groups, or class projects; help encourage access to follow-up supports; and help support a positive school and community culture that is actively engaged in developing healthy relationships.*

As discussed above in terms of responses to individual cases, *educational approaches will also be more impactful if they focus on relational harm rather than legal consequences.* A 2016 agent described providing educational presentations that are quite focused on legal warnings: "[we educate] the young people about […] cyberbullying and the law, […] about online safety and [making them] aware there is a law" (CS2). Agents in 2020 described presentations that were somewhat more balanced between discussing harm and providing legal education, however educational approaches may still lean too heavily on legal scare tactics by sometimes including police officers as co-presenters and focusing more on legal warnings than relational impacts (CS5). As one of the restorative justice experts explained, *presentations focused on legal warnings may have immediate impacts by scaring youth into compliance, but are less likely to effect long term behavioural change (RA1).* Impactful education must go beyond making youth "afraid of punishment", and should rather help youth put themselves "in another person's shoes".[57] *An overemphasis on the law could also backfire in several ways; For instance, youth victims of cyberbullying or nonconsensual distribution may be less likely to seek support if they believe it will necessarily become a "big deal" by starting a legal process or leading to the criminalization of their peers* (Choo, 2015; Dodge & Lockhart, 2021).

Both the cyber safety model and a focus on legal impacts can sometimes leave young people feeling fearful and unempowered. However, education experts assert that educational interventions should instead help young people feel empowered to make positive change, to find supports when they are in need, and to support others (Johnson, 2016). As Nik Basset, Education and GSA Coordinator for the Youth Project states, young people should leave an educational workshop feeling empowered to make their school and community better (e.g. to start a GSA or student club that addresses oppressive cultures in their school and community) and more equipped to support themselves or a peer that is struggling (e.g. knowledge of supports and ideas about how to search for additional resources), rather than leaving feeling hopeless or scared[58]. For example, a workshop

[57] https://mediasmarts.ca/sites/default/files/lesson-plans/lesson_promoting_ethical_behaviour_online_0.pdf

[58] Personal communication, March 2021.

about gender identity could end with questions such as: How would you support a friend that is being bullied for being trans? What could you say to help them feel better? Where might you find helpful resources for them online or in the community? *In a well-intentioned attempt to protect young people, "cyber safety" presentations often describe horror stories of digital harm to try to scare youth away from risky behaviour, but it is necessary to recognize that youth will encounter challenges, make mistakes, and take risks and they, therefore, also need to be supported to imagine what it looks like when someone who is harmed is well-supported and to consider what their role could be in providing positive supports.* Education should help young people normalize supportive behaviour[59] and help them understand that they "have the ability to make practical contributions in responding to incidents of cyberbullying, such as by taking steps to denounce bullying rather than being a complicit bystander, or to help bullying victims after the fact by reassuring them that the treatment they received from the bully was inappropriate" (*Cyberbullying Hurts*, 2012, p. 58). Youth should also be informed that, while harm can occur online, the online world has also allowed young people access to a multitude of supports and resources and is often a place for, especially marginalized, youth to find supportive communities (Mishna et al., 2018).

Recommendation #25: CyberScan should move away from the "cyber safety" model of education and should instead seek to addresses the core discriminatory and relational issues that underly cyberbullying and nonconsensual distribution. Addressing these core issues will require ongoing and interactive education on healthy/ethical relationships, diversity /inclusion, consent, and empathy.

Recommendation #26: The province should ensure adequate resourcing of government and community organizations that can help support the need for engaging and impactful education to prevent digital harms.

Recommendation #27: To ensure education is relevant to particular school contexts and allows youth to access continued support in their communities, educational approaches should be cocreated with school staff or community organizations that young people are familiar with and can easily access for ongoing support.

Recommendation #28: Educational approaches should avoid an over-reliance on legal warnings and scare tactics, and instead help youth feel empowered to make change, seek support, and support others.

EDUCATION REGARDING NONCONSENSUAL INTIMATE IMAGE DISTRIBUTION

CyberScan's educational approach to the issue of nonconsensual intimate image distribution requires individual focus. Because nonconsensual distribution is a form of sexual violence, it is particularly important for education on this topic to be informed by best practices and to avoid

[59] https://mediasmarts.ca/digital-media-literacy/digital-issues/online-ethics

victim blaming/shaming narratives (Fairbairn et al., 2013). *When asked about their approach to education on nonconsensual intimate image distribution, CyberScan agents primarily described education aimed at changing the behaviours of those who consensually share images (i.e. targeting the behaviours of potential victims rather than potential perpetrators of harm).* As an agent in 2016 stated:

> “We explain about potential consequences of sexting in the future, […] how these photos can pop up five, ten years down the road too, you know. We talk about how once you take that intimate image of yourself on an electronic device and you hit that send, you don’t have control of that photo anymore. We use an example, that sexting is like going to Costco or Walmart and asking them to print 1000 photos of you naked and walking around handing these photos out to people. We ask ‘Would you do that?’ and they of course all go ‘No’, but if you hit that send button one time thousands of people can end up having copies of it” (CS2).

By asserting that trusting someone with your nude image is the equivalent of purposefully handing out one’s nude image to strangers, this example ignores the actions of perpetrators of nonconsensual distribution (who violate a person’s trust, privacy, and bodily autonomy through their actions) and instead focuses the blame on the consensual act of the victim (and frames the victim’s act as stupid/naive and worthy of shaming). Scholars have found that education campaigns directed at the potential victim’s behaviour can act to affirm the harmful belief that victims of this act are “bad, dirty, stupid and/or dangerous” (Albury et al., 2017; Angelides, 2013; Naezer & Oosterhout, 2021, p. 7). That is, *education that focuses primarily on the consensual image creator can reinforce rather than challenge harmful victim blaming/shaming beliefs and normalize the culture that condones nonconsensual distribution.*[60]

CyberScan’s current educational presentations include a video, titled *Teen Voices: Sexting, Relationships, and Risks*[61], that likewise ignores the actions of perpetrators and treats nonconsensual distribution as the inevitable consequence of trusting others. This video features several teens sharing their feelings about nonconsensual intimate image distribution. The teens consistently talk about images “getting leaked” or getting “sent around” without acknowledging that someone chose to do this and that these nonconsensual acts are what caused the harm. While showing this kind of video[62] may seem like an appropriate way to share the “voices of youth”, the perspectives youth provide in these kinds of videos may simply echo the victim blaming and scare tactic messaging that they receive from ill-advised educational presentations (Angelides, 2013). *Education about nonconsensual distribution must challenge the idea that this act is inevitable and, instead, assert that the culture that normalizes nonconsensual acts is changeable and that we can all help support a culture that values consent and respects bodily autonomy.*

[60] https://mediasmarts.ca/blog/sexting-shifting-focus-victim-blaming-respect-consent

[61] https://www.youtube.com/watch?v=IZwVT6WnPQY

[62] A video with a similar problematic approach was recently created by the Nova Scotia RCMP: https://www.halifaxtoday.ca/police-beat/high-school-students-team-up-with-rcmp-to-create-videos-on-dangers-of-sharing-intimate-images-video-3290301

To avoid victim blaming/shaming and to teach youth the importance of consent and bodily autonomy, educational responses need to acknowledge that consensual image sharing is not inherently harmful (Albury et al., 2017; Karaian, 2014) and, rather, that harm occurs when images are shared without consent or within a context of coercion. As teens (and adults for that matter) often report consensually sharing images for fun or to flirt, and many images that are consensually shared remain confidential (Lee & Crofts, 2015; Steeves, 2014), nonconsensual distribution should not be normalized as the inevitable result of trusting others. Rather, *scholars recommend teaching young people that, like others sexual acts, intimate image sharing must only occur when there is consent (Albury et al., 2017; Hasinoff, 2015; Shariff & DeMartini, 2015).* Starting with the importance of consent, education can then focus on challenging the beliefs that might make people believe it is okay to share an image without consent[63] or to shame/blame a victim of nonconsensual distribution. Educators could also explain that in many of the most tragic cases of nonconsensual distribution, such as the Rehtaeh Parsons case, the harm experienced by the victim was amplified by bystanders who bullied the victim rather than offering support; Students could then brainstorm the best ways to support a victim. Young people could also brainstorm practical tips to ensure they don't share someone's image without consent (e.g. delete images after a short period so that you do not risk violating someone's privacy at a later date when you might be drunk/mad/or pressured by friends and ensure your images are not being auto uploaded to other devices or the cloud).

WHEN YOU PRESSURE ME FOR NUDE PICS,
I THROW UP IN MY MOUTH A LITTLE.
THATSNOTCOOL.COM

Although the victim responsibilizing / "anti-sexting" approach was once popular, many youth-serving organizations have since recognized that this approach is counterproductive as it leads to increased shaming and blaming of victims, can make victims less likely to seek support, does not teach the importance of consent, and does not teach youth safer-sexting tips[64] (Dodge & Lockhart, 2021; Fairbairn et al., 2013). There are now many resources available that CyberScan could use to provide a consent-focused approach.[65] Telus and MediaSmarts[66], Kids Help Phone[67], and Webwise.ca[68] all provide consent-focused education that does not shame consensual sexting. The website thatsnotcool.com provides examples (such as the image on the right) of education campaigns that instead target nonconsensual or coercive behaviour and are meant to empower youth to "set boundaries and make informed decisions" (Fairbairn et al., 2013, p. 52). Education should also help youth feel safe reaching out for support and feel that there are ways adults can help them (e.g. CyberScan can report/remove images posted online or contact the person who shared the image to have them delete it from their device). Education should also help youth feel empowered to support a peer whose image is shared without consent (e.g. refuse

[63] For example, recognizing that boys sometimes nonconsensually share images of girls to impress other boys, educators could help youth think critically about pressures on boys to prove their masculinity and sexual experience (Ringrose & Harvey, 2015).

[64] Teaching youth tips to sext more safely (as with safer-sex advice) does not amount to encouraging them to sext, but rather gives them knowledge and tools to make more informed choices and to feel they can come to adults for non-judgemental support.

[65] https://www.youtube.com/watch?v=8pqnL2-7MwU

[66]https://mediasmarts.ca/sites/default/files/guides/guide_taking_youth_about_forwarding_sexts.pdf

[67] https://kidshelpphone.ca/get-info/what-sexting

[68] https://webwise.ca/cyber-101/sexting/

to share the image, tell the person who shared it without consent that it is not okay, tell the victim you think what happened to them is wrong and you are there for them, help the victim find additional resources or supports).

Finally, CyberScan should ensure that the education they provide corrects rather than reaffirms misconceptions about nonconsensual intimate image distribution. In the *Teen Voices, Sexting, Relationships, and Risks* video that CyberScan shows youth, it is implied that youth victims of nonconsensual intimate image distribution are almost always girls. Contrary to this popular assumption, Canadian research has found that teen boys are actually slightly more likely to be victims of this act than girls (Steeves, 2014). While boys and girls experience similar rates of victimization, education should discuss the discriminatory beliefs that can lead to girls being judged more harshly when their images are shared without consent.[69] The *Teen Voices* video includes youth describing this increased impact on girls (e.g. "getting busted for sexting is more embarrassing for girls than guys" and "it's so easy as a female to have your reputation thrown away"[70]), but it does not help youth understand and challenge the discriminatory reasons why this is the case and, therefore, simply reaffirms this as "the way it is". Educators should also challenge the idea that all cases of nonconsensual intimate image distribution end in tragedy for the victim. For instance in the *Teen Voices, Sexting, Relationships, and Risks* video, many of the teens express that images will be spread all over the internet and will impact your life/reputation forever: "When a nude gets leaked like, your family gonna see it, different people you don't even know screen shotting you, the picture that you sent to this one person is never going to go away, it's never going to, you're just stuck with it. […] [your] whole body is all over the internet and now everybody's seeing [you]"[71]. Contrary to this worst-case scenario, in many cases nonconsensually distributed images are not made publicly available but are rather shared between youth through text or messaging apps (Walker & Sleath, 2017) and are likely to be deleted on request from a CyberScan agent, school official, or parent/guardian. Additionally, even if images are widely and publicly distributed, youth should be made aware of the many supports that can help control the spread of the images (e.g. most major social media companies will remove the image and tag it as a nonconsensually shared intimate image and Google will delist images shared without consent from its search engines) and the supports that are available to help deal with resulting harms (e.g. emotional support from school counsellors, Kids Help Phone, or CyberScan). It is important to reassure youth victims rather than sending messages that confirm the idea that they should panic and that they will be unable to ever recover from this harm (See: Image/content takedown and technological know-how).

Recommendation #29: Education on nonconsensual intimate image distribution should avoid a victim responsibilization (i.e. anti-sexting) focus and, instead, focus on the importance of consent and bodily autonomy.

Recommendation #30: CyberScan must ensure that their educational messaging challenges rather than reaffirms common misconceptions about nonconsensual intimate image distribution.

[69] https://mediasmarts.ca/blog/sexting-shifting-focus-victim-blaming-respect-consent
[70] https://www.youtube.com/watch?v=IZwVT6WnPQY
[71] https://www.youtube.com/watch?v=IZwVT6WnPQY

LABELLING YOUTH INTIMATE IMAGES AS "CHILD PORNOGRAPHY"

CyberScan's educational presentations, like many police-led educational initiatives in Canada, tell youth under the age of 18 that they have committed child pornography offences if they have consensually and privately shared an intimate image of themselves with a peer. This framing of youths' consensual intimate image sharing as child pornography is concerning, as the law is much less straight forward on this point than CyberScan agents seem to imply to youth. In Canada, a young person has never been convicted for sharing an intimate image of themselves with a peer (i.e. sexting), and many legal scholars believe they likely never will be / should never be (Karaian & Brady, 2020). In *R v Sharpe* (2001), the Supreme Court of Canada stated that youth who consensually and privately create sexual images of themselves or themselves with their partner should be excluded from child pornography offences. In *Sharpe*, the majority decision states that this kind of consensually made and privately held intimate image could be "of significance to adolescent self-fulfillment, self-actualization and sexual exploration and identity"[72]. Although this decision was made before popular knowledge of "sexting" as it is now understood (Karaian & Brady, 2020), it remains unlikely that consensual youth sexting will ever be charged as child pornography because no harm has occurred in such a case. The harm occurs when intimate images are shared without consent, and it is then that charges may be used (and have been used) against a youth who has *nonconsensually* shared an image of someone.

Although warnings of child pornography charges for consensual sexting are likely a well-intentioned attempt to reduce the risk of nonconsensual distribution, in practice this scare tactic approach is unlikely to reduce rates of consensual sharing; Instead, it acts to send the harmful message that victims of nonconsensual distribution have done something wrong/immoral/illegal. This messaging acts to reaffirm harmful victim blaming/shaming beliefs and can make victims of nonconsensual intimate image distribution less likely to seek support due to fears of being criminalized or judged (*Cyberbullying Hurts*, 2012; Dodge & Lockhart, 2021; Fairbairn et al., 2013; Naezer & Oosterhout, 2021). CyberScan agents report that parents and school officials often ask them to respond to youth who have consensually created an intimate image of themselves or have consensually shared an intimate image with a partner or friend (CS2; CS5; CS6). While CyberScan agents report that they sometimes have one-on-one discussions with these consensual image creators/sharers in which they tell them that they could be charged with child pornography offences for both of these acts, it is clear in the law that self-created and privately held intimate images *are not* included within the scope of child pornography offences and it is unlikely that consensual sexting will be charged as child pornography either.

Many educational resources for youth in Canada now recognize that "sexting can be a healthy way for young people to explore sexuality and intimacy when it's consensual"[73] and that educational responses should focus on highlighting the harm and legal consequences of acts committed *without consent*. While CyberScan's responses do not currently embrace this model, *the way in which CyberScan uses warnings of child pornography offences in response to consensual sexting does vary in forcefulness depending on the agent delivering the message.* One agent in 2016 reported using explicit warnings of child pornography offences:

[72] R v Sharpe, 2001 SCC 2, para 109.
[73] https://mediasmarts.ca/digital-media-literacy/digital-issues/sexting

> “[I tell youth], if you are taking a photograph of yourself and you are under the age of 18, you’ve just made child pornography. If you’re sharing it, you’ve now distributed child pornography. If someone is receiving it, they are in possession of child pornography. And those are serious criminal code offences. So we would talk to them about that. Now, between you and I, there is some discretion there with the police, but we wouldn’t bring that up with the youth. If police are seeing that a girl has shared a video of herself with a boyfriend and the parents found it, you know the police aren’t [going to charge her] because the harm was not there… they didn’t share it with the world, they were sharing it between themselves. Yes it is absolutely illegal for them to do that, but in reality the response will be to just get them to delete and remove [the images], that would be the appropriate approach when you are dealing with that type of situation” (CS4).

Although this agent was aware that police use discretion not to charge youth for consensual acts (though was seemingly unaware of the legal precedent that complicates a straightforward reading of child pornography laws), they nonetheless explicitly threatened youth who engage in consensual acts with child pornography offences. This kind of education is likely to create anxiety for youth who have already consensually shared images, and it also sends the message that victims of nonconsensual distribution should avoid seeking support from adults as they risk criminalizing themselves. On the other hand, youth may simply tune out this message as they may know from experience that those in their school who have been found consensually sexting were not criminalized with child pornography charges.

A second agent in 2016 described taking a somewhat more balanced approach that told youth that “if you’re a young person in Canada under the age of 18 and you take a naked photo of yourself, technically you’re in possession of child pornography. [But if someone shares your image without consent and] you come and give us the information, you’re not going to get in trouble. We are going to help you” (CS2). While this kind of explanation may be less likely to discourage victim reporting, consensual youth sexters and victims of nonconsensual distribution still hear the message that they have *technically* committed a criminal offence and, therefore, they may still avoid seeking adult supports. A 2020 agent explained a similar approach, “[we tell youth that] even taking a picture of themselves is illegal […] it is technically child pornography. But I tell them the police are there to help, they are not going to charge you for trying to help, […] if you are a victim of this they are not going to charge you with making child pornography because you took a picture of yourself” (CS5). While this approach is certainly better than the forceful use of criminal offences as a scare tactic to try to stop consensual image creation and sharing, this kind of messaging is likely to leave youth confused and uncomfortable seeking adult supports. And, again, it wrongly states that even creating and privately keeping a nude image of yourself is child pornography despite the decision in *Sharpe*. The complexity of child pornography laws in relation to youth’s consensually shared intimate images leave CyberScan agents in a difficult spot in terms of some of their messaging. Educational messaging about youths’ consensual intimate image sharing would certainly be easier if child pornography offences were clarified to more explicitly exclude consensual contexts between close in age youth; However, *there is no reason to believe that consensual youth sexting will suddenly start to be charged as child pornography and, therefore, many educational initiatives for youth in Canada now discuss consensual intimate image sharing as a sexual act that, like all sexual acts, has both risks and rewards but is not* *inherently wrong or harmful.* CyberScan should consider implementing this kind of non-judgemental and sex-positive approach to education about intimate images, as this approach is now widely recognized as the most evidence-informed approach and has been taken up by organizations such as Kids Help Phone[74], Webwise.ca[75], and MediaSmarts[76]. All of these resources discuss the many legitimate reasons a youth might choose to create or share intimate images and, thereby, create an opening to non-judgmentally discuss the risks/rewards, tools to sext more safely, and the importance of consent. These resources also all explain the details of the legal context of intimate image sharing for youth in Canada, but they highlight that close-in-age youth who share images consensually will likely not be charged as child pornographers and that what is most important is to respect the consent and privacy of others.

As much as possible, CyberScan should move away from a focus on child pornography laws. This is true even when discussing nonconsensual acts of intimate image distribution. As child pornography offences were "created to protect children from sexual exploitation" by adults, many scholars, police officers, and judges[77] in Canada have expressed that it is inappropriate to frame nonconsensual intimate image distribution among youth as "child pornography" (Dodge & Spencer, 2018; Shariff & DeMartini, 2015, p. 295). With the more appropriate offence of nonconsensual intimate image distribution now available to charge both youth and adults who share images without consent, it is possible to discuss the potential legal consequences of nonconsensual distribution without referring to the ill-suited and overly-stigmatizing offence of child pornography. As Segal describes in his review of the Rehtaeh Parsons case:

> "Many would agree that charging youths with child pornography-related offences is an unintended use of the Criminal Code's child pornography provisions. While there is a valid debate to be had on that issue, the question no longer needs to be decisively answered in light of the new criminal offences relating to distributing or making available intimate images without consent. While the child pornography offences remain available in cases like this one, these new offences would cover most instances where young persons distribute images of a sexual nature without consent, and they are arguably a better way of addressing cases where all involved are youth" (Segal, 91).

While nonconsensual intimate image distribution can rightly be said to be "technically child pornography", there is little utility in discussing this technicality with young people when they can instead be made aware of the offence of nonconsensual intimate image distribution.

Avoiding a child pornography framing for both consensual and nonconsensual intimate image sharing among youth would be easier if the provincial government provided further clarity on how mandatory child pornography reporting requirements apply to cases among youth. Currently, CyberScan agents interpret the mandatory duty to report child pornography[78] to the police as including all cases of consensual and nonconsensual intimate image distribution among youth,

[74] https://kidshelpphone.ca/get-info/what-sexting
[75] https://webwise.ca/cyber-101/sexting/
[76] https://mediasmarts.ca/digital-media-literacy/digital-issues/sexting
[77] R v SB et al., 2014 BCPC 0279; R v Zhou, 2016 ONCJ 547.
[78] In cases reported to CyberScan by schools, the case is often already reported to the school resource officer by the principal, so CyberScan is not required to call police themselves (CS5).

even if there is no evidence that the images have been shared in a public manner that would put them at risk of falling into the hands of an adult who would view them for a sexual purpose. Although this duty to report was created, as were child pornography charges, to address adults who sexually exploit children, CyberScan agents explained that: "If we […] get a call that there was a mutual relationship between youth and they exchanged images and so on, we would still have to check that that is reported to local police, and then they would deal with that whatever way they felt necessary. But I would have to make sure it was at least reported, just because that's my duty to report. I'm bound under a duty to report child pornography […]" (CS5). CyberScan agents explained that police seem to perceive these reports of image share among youth as an unnecessary nuisance, as the reason this duty to report exists is to make police aware of a child in danger of sexual exploitation at the hands of an adult: "I do have a duty that it has to be reported to the police. Now the police most times don't do anything about it, because that's the last thing they want to do, and actually they don't want to even hear it when we have to call. The police don't want to deal with that [as child pornography] right, but I think we have that legal obligation" (CS5). Although some cases of nonconsensual distribution could include public online sharing that risks images being added to online child pornography caches viewed by adults, it seems particularly unnecessary for cases to be reported in the many instances in which images are nonconsensually distributed among a particular group of youth (via showing images to others on a phone, sending to a private group message, or texting) (Walker & Sleath, 2017) and there is little chance of images somehow ending up in the hands of an adult abuser. The duty to report should be clarified, as there seems to be no purpose to reporting images as "child pornography" in cases of consensual sexting among youth (i.e. images have remained private between youth) or in cases of nonconsensual intimate image distribution where images have not been made publicly accessible (i.e. images have been shared nonconsensually but only to other youths). *Despite the challenges created by mandatory child pornography reporting policies and a complicated legal landscape, CyberScan's education materials and responses should refrain from framing this act as "child pornography" whenever possible. When youth are told they have committed child pornography or are child pornographers, it can create confusion and undue stigma*[79] *and decrease the likelihood that victims of nonconsensual distribution will seek support*. The current challenges in avoiding a child pornography framing speak to the importance of gaining further clarity from the courts or federal government regarding the use of child pornography offences in cases that do not involve adult abuse of children.

Recommendation #31: CyberScan should avoid framing consensual intimate image creation/sharing and nonconsensual intimate image distribution among youth as "child pornography" whenever possible.

Recommendation #32: CyberScan (as well as police and school officials) should ensure that they fully understand the limitations on how child pornography offences can be applied, as determined in R v Sharpe (2001), and recognize that these offences are ill-suited (and increasingly avoided) in legal responses to cases among youth.

[79] See *R v SB et al.* (2014) for one example of the negative impacts that can come from framing youth nonconsensual distribution as child pornography

Recommendation #33: The provincial government should review the duty to report child pornography to determine whether the duty to report applies to cases of intimate image sharing among youth in which there is little risk of the images being used as child pornography by an adult.

INFORMING NATIONAL RESPONSES TO DIGITAL HARM

This report has detailed several ways in which the CyberScan unit could improve its responses to cyberbullying and nonconsensual intimate image distribution. However, *the core supports provided through CyberScan's support line role (i.e. technological and emotional support for complainants) is a positive and in-demand resource. CyberScan's work in this regard should be used as a model to provide all Canadians with this kind of support line.* CyberScan agents in both 2016 and 2020 asserted that a national resource akin to CyberScan is needed to allow all Canadians to receive support in response to digital harms: "Here in Nova Scotia there is a place you can call, but in other places there is nowhere that you can even call about some of this stuff. Like if you go to the police and they can't help you, well at least here you can give us a call. And we're paid to research and kind of see how we can help, so it's a start and we need a lot more, but it's a start" (CS5). Some agents also asserted that a national program would allow for more comprehensive educational resources to be made available to Canadians, citing the breadth of resources available in other countries such as Australia: "Australia they have this national eSafety Commissioner and they have so many resources on there, and I wish that Canada had something like that, some sort of national organization that is there to help Canadian's have a safer experience online. […] I'd love to be able to offer more resources and things like that if we had the money… again I just look at the site for Australia and they have […] stuff for seniors, they have stuff for intimate image abuse, they have stuff for cyberbullying, they have stuff for newcomers" (CS5). A national strategy should allow all Canadians to access immediate emotional/informational supports and assistance with takedown/deletion of cyberbullying content and nonconsensually distributed intimate images and should also act as a hub for education, prevention, and support resources. Somewhat comparable services are available in the UK through the Revenge Porn Helpline and in Australia through the national eSafety Commissioner, but Canada does not currently have a national program to provide supports and resources. If a national support line and resources hub were to be created, it would be important to include a strategy for community-based organizations that can engage in preventative education and restorative responses in a more localized way as well. *The evidence of CyberScan's successes and the recommendations for their improvement should both provide important information for the federal government as they continue to consider ways to address digital harms in Canada.*

Recommendation #34: Lessons learned from the CyberScan unit should be shared with the federal government to push for national supports that bring together the best aspects of CyberScan with additional resourcing for all Canadians.

REFERENCES

Albury, K., Hasinoff, A., & Senft, T. (2017). From Media Abstinence to Media Production: Sexting, Young People and Education. In L. Allen & M. L. Rasmussen (Eds.), *The Palgrave Handbook of Sexuality Education* (pp. 527–545). Palgrave Macmillan.

Angelides, S. (2013). 'Technology, hormones, and stupidity': The affective politics of teenage sexting. *Sexualities, 16*(5–6), 665–689.

Beran, T., Mishna, F., McInroy, L., & Shariff, S. (2015). Children's Experiences of Cyberbullying: A Canadian National Study. *Children and Schools*, *37*(4), 207–215.

Boyd, A. (2020, June 22). Should we have cops in schools? Why other districts are now asking Toronto. *Toronto Star*.

Boyd, D. (2014). *It's complicated: The social lives of networked teens*. Yale University Press.

Choo, H. (2015). Why we are still searching for solutions to cyberbullying: An analysis of the North American responses to cyberbullying under the theory of systemic desensitization. *University of New Brunswick Law Journal*, *66*, 52–77.

Cooke, A. (2021, May 18). Father of Rehtaeh Parsons looks to 'turn a page' in writing book about his daughter. *Global News*.

Crofts, T., & Lievens, E. (2018). Sexting and the law. In *Sexting: Motives and risks in online sexual self-presentation* (pp. 119–136). Palgrave MacMillan.

Cyberbullying Hurts: Respect for Rights in the Digital Age. (2012). Report: Standing Senate Committee on Human Rights, Ottawa.

Dodge, A. (2021). 'Try Not to be Embarrassed': A Sex Positive Analysis of Nonconsensual Pornography Case Law. *Feminist Legal Studies*, *29*(1), 23–24.

Dodge, A., & Lockhart, E. (2021). "Young People Just Resolve it in Their Own Group": Youth Perspectives on Criminal Responses to Nonconsensual Pornography. *Youth Justice*, *Online First*.

Dodge, A., & Spencer, D. (2018). Online Sexual Violence, Child Pornography or Something Else Entirely? Police Responses to Non-Consensual Intimate Image Sharing among Youth. *Social & Legal Studies*, *27*(5), 636-657.

Fairbairn, J., Bivens, R., & Dawson, M. (2013). *Sexual violence and social media: Building a framework for prevention*. Report: OCTEVAW, Ottawa.

Fraser, D. (October 20, 2017). Letter to Nova Scotia Legislature, Law Amendments Committee: https://nslegislature.ca/sites/default/files/pdfs/committees/63_1_LACSubmissions/20171023/20171023-027-003.pdf.

Hamilton, A. (2018). Is Justice Best Served Cold?: A Transformative Approach to Revenge Porn. *UCLA Women's Law Journal*, *25*(1), 1–44.

Hasinoff, A. A. (2015). *Sexting panic: Rethinking criminalization, privacy, and consent*. University of Illinois Press.

Henry, N., Flynn, A., & Powell, A. (2018). Policing image-based sexual abuse: Stakeholder perspectives. *Police Practice and Research*, *19*(6), 565–581.

Henry, N., Powell, A., & Flynn, A. (2017). Not just 'revenge pornography': Australians' experiences of image-based abuse. Report: RMIT University, Melbourne.

Johnson, M. (2016). Digital literacy and digital citizenship: Approaches to girls' online experiences. In J. Bailey & V. Steeves (Eds.), *EGirls, eCitizens* (pp. 339–360). University of Ottawa Press.

Karaian, L. (2014). Policing 'sexting': Responsibilization, respectability and sexual subjectivity in child protection/crime prevention responses to teenagers' digital sexual expression. *Theoretical Criminology*, *18*(3), 282–299.

Karaian, L., & Brady, D. (2020). Revisiting the "Private Use Exception" to Canada's Child Pornography Laws: Teenage Sexting, Sex-Positivity, Pleasure, and Control in the Digital Age. *Osgoode Hall Law Journal*, *56*(2), 301–349.

Khoo, C. (2021). *Deplatforming misogyny: Report on platform liability for technology-facilitated gender-based violence*. Report: LEAF, Ottawa.

Lee, M., & Crofts, T. (2015). Gender, Pressure, Coercion and Pleasure: Untangling Motivations for Sexting Between Young People. *The British Journal of Criminology*, *55*(3), 454–473.

Llewellyn, J., Archibald, B. P., Clairmont, D., & Crocker, D. (2014). Imagining Success for a Restorative Approach to Justice: Implications for Measurement and Evaluation. *Dalhousie Law Journal*, *36*(2), 281–316.

McGlynn, C., Rackley, E., & Houghton, R. (2017). Beyond 'Revenge Porn': The Continuum of Image-Based Sexual Abuse. *Feminist Legal Studies*, *25*(1), 25–46.

Mishna, F., Regehr, C., Lacombe-Duncan, A., Daciuk, J., Fearing, G., & Van Wert, M. (2018). Social media, cyber-aggression and student mental health on a university campus. *Journal of Mental Health*, *27*(3), 222–229.

Mishna, F., Schwan, K. J., Birze, A., Van Wert, M., Lacombe-Duncan, A., McInroy, L., & Attar-Schwartz, S. (2020). Gendered and Sexualized Bullying and Cyber Bullying: Spotlighting Girls and Making Boys Invisible. *Youth & Society, 52*(3), 403–426.

Mishna, F., & Van Wert, M. (2015). *Bullying in Canada*. Oxford University Press.

Morrison, B. (2002). Bullying & Victimisation in Schools: A Restorative Justice Approach. *Trends & Issues in Crime & Criminal Justice*, *219*, 1–7.

Naezer, M., & Oosterhout, L. van. (2020). Only sluts love sexting: Youth, sexual norms and non-consensual sharing of digital sexual images. *Journal of Gender Studies*, Online First.

Palmeter, P. (2017, October 20). Privacy lawyer who challenged cyberbullying law worries new bill swings too far. *CBC*.

Powell, A., & Henry, N. (2017). *Sexual violence in a digital age*. Palgrave Macmillan.

Reynolds, A. (2021, March 22). Indigenous women from across Mi'kma'ki fighting back against men sharing their images without consent. *SaltWire*.

Ringrose, J., & Harvey, L. (2015). Boobs, back-off, six packs and bits: Mediated body parts, gendered reward, and sexual shame in teens' sexting images. *Continuum*, *29*(2), 205–217.

Russell, S., & Crocker, D. (2016). The institutionalisation of restorative justice in schools: A critical sensemaking account. *Restorative Justice*, *4*(2), 195–213.

Segal, M. (2015). *Independent Review of the Police and Prosecution Response to the Rehtaeh Parsons Case*. Report: Murray D Segal Professional Corporation.

Shariff, S., & DeMartini, A. (2015). Defining the Legal Lines: EGirls and Intimate Images. In J. Bailey & V. Steeves (Eds.), *EGirls, eCitizens* (pp. 281–305). University of Ottawa Press.

Steeves, V. (2014). *Young Canadians in a wired world, phase III: Sexuality and romantic relationships in the digital age*. Report: MediaSmarts.

Taylor, J. (2016). Minding the gap: Why and how Nova Scotia should enact a new cyber-safety act. *Canadian Journal of Law and Technology, 14*, 157–171.

Tutton, M. (2018, July 5). New cyberbullying law can force removal of intimate images online. *CBC.*

Vitale, A. (2017). *The End of Policing*. Verso.

Wachtel, T. (2016). *Defining Restorative*. Report: International Institute of Restorative Practices.

Walker, K., & Sleath, E. (2017). A systematic review of the current knowledge regarding revenge pornography and non-consensual sharing of sexually explicit media. *Aggression and Violent Behavior, 36*, 9–24.