2022

Submission to the Province of Nova Scotia on Its Review of the Intimate Images and Cyber-Protection Act - LEAF

Suzie Dunn

Rosel Kim

LEAF FAEJ

WOMEN'S LEGAL EDUCATION & ACTION FUND

FONDS D'ACTION ET D'ÉDUCATION JURIDIQUE POUR LES FEMMES

Submission to the Province of Nova Scotia on its review of the *Intimate Images and Cyber-protection Act*

28 January 2022

Written by: Suzie Dunn and Rosel Kim[1]

[1] Suzie Dunn is an Assistant Professor at Dalhousie University's Schulich School of Law and a member of LEAF's Technology-Facilitated Violence Advisory Committee. Rosel Kim is a Staff Lawyer at the Women's Legal Education and Action Fund. We would also like to thank Alexa Dodge, Pam Hrick, Emily Laidlaw, Wayne MacKay, and Molly Reynolds for their contributions in reviewing this submission.

Public Safety & Security Division
Department of Justice
Government of Nova Scotia
iicpa@novascotia.ca

[*delivered electronically*]

Introduction

The Women's Legal Education and Action Fund (LEAF) commends the Nova Scotia government for reviewing its *Intimate Images and Cyber-protection Act* (the *Act*) and seeking public input for this review. Nova Scotia has been, and continues to be, a leader in Canada for its role in advancing innovative laws and supports for people targeted by technology-facilitated violence (TFV), digital abuse, and the non-consensual distribution of intimate images (NCDII). As these forms of harmful behaviour evolve and become better understood, it is important to revisit this legislation to assess whether it is providing meaningful and accessible responses to such serious social harms. This consideration is especially important for equality-deserving groups who often experience the brunt of abusive behaviour online.

LEAF recognizes that these forms of harms disproportionately impact historically marginalized communities. Women, girls, and gender-diverse people, particularly those with intersecting marginalized identities, including Indigenous, Black, people of colour, members of 2SLGBTQQIA communities, and people with differing abilities, face higher rates of targeted attacks that focus on their gender, race, sexual orientation, gender identity, gender expression, and ability. These attacks can have devastating consequences on the health and wellbeing of those targeted.

About LEAF and its Expertise

LEAF is a national, charitable, non-profit organization that works towards advancing substantive gender equality through litigation, law reform, and public education. Since 1985, LEAF has intervened in over 100 cases – many of them before the Supreme Court of Canada – that have advanced equality in Canada.

In recent years, LEAF has been involved in addressing law reform in relation to technology-facilitated gender-based violence (TFGBV) across Canada. Harmful digital conduct such as online hate, harassment, and the non-consensual distribution of intimate images (NCDII) have a disproportionately detrimental impact on women and gender-diverse people, especially those in leadership roles and those who speak up about equality issues online.[2] These harms impact their

[2] Sharon Goulds et al "Free to Be Online" (Plan International, 2020); Azmina Dhrodia, "#Toxic Twitter: Violence and Abuse Against Women Online" (London, UK: Amnesty International, 2018); "Measuring the Prevalence of Online Violence Against Women" (2021) The Economist Intelligence Unit; "Methodology: Measuring the Prevalence of Online Violence against Women" (2021) The Economist Intelligence Unit; Rosel Kim & Cee Strauss, "Of Commitment

ability to express themselves and participate in digital spaces, significantly stifling their fundamental freedoms of thought, belief, opinion and expression. However, these harms are not limited to the digital realm. They can impact a person's mental health, ability to find work, physical safety, personal reputation, and their capacity to maintain relationships, among other things.[3] All people deserve to engage safely in the online spaces that have become crucial to all aspects of our lives. They should not face devastating repercussions for participating in the digital public sphere.

To date, LEAF has made multiple submissions to various levels of government on issues related to equality and technology. This includes its 2019 submission to the House of Commons Standing Committee on Justice and Human Rights' study of online hate; its 2021 submission to Canadian Heritage on the Federal Government's proposed approaches to address harmful content online; and its most recent submission to the Toronto Police Board on its draft policy for the Use of Artificial Intelligence in December of 2021.

LEAF has developed expertise in the gendered impact of online harassment, hate speech, and the non-consensual distribution of intimate images, as well as other forms of TFGBV. It's Technology-Facilitated Violence Advisory committee is made up of many of Canada's leading experts in the areas of TFGBV, including online harassment and NCDII. In 2019, LEAF intervened in the landmark case of *R v Jarvis*, where it urged the Supreme Court of Canada to apply an equality lens when interpreting the *Criminal Code* provision of voyeurism. In April 2021, LEAF released a research report titled "Deplatforming Misogyny", authored by human rights and technology lawyer Cynthia Khoo. This report examines how digital platforms can be held accountable and liable for their role in perpetuating TFGBV from a substantive equality perspective. It provides an overview of TFGBV and many of the legal issues that surround it, including freedom of expression. This report also provides recommendations to governments on what service they should provide to the public, including research, education, resources to front-line organizations, and statutorily mandated bodies who can provide direct support to those targeted by TFGBV.

Below we will provide recommendations on changes to the *Act* and its regulations, as well as recommendations on aspects of CyberScan. This submission relies on and builds on previous recommendations made in LEAF's Deplatforming Misogyny report, the *Uniform Non-Consensual Disclosure of Intimate Images Act*, and Alexa Dodge's Deleting Digital Harm: A Review of Nova Scotia's CyberScan Unit report. Our recommendations focus on providing more expedient and direct supports to those experiencing TFV and NCDII; expanding the scope of the definition of intimate images and reconsidering the parameters of "public interest"; and broadening the scope of research and educational materials to ensure that they are survivor-centric and to cover the systemic and social context that results in digital abuse and NCDII.

---

and Precarity: Community-Based Approaches to Addressing Gender-Based Online Harm" in Anastasia Powell, Asher Flynn, & Lisa Sugiura, eds, *The Palgrave Handbook on Gendered Violence and Technology* (London: Palgrave Macmillan) 607-629.

[3] Samantha Bates, "Revenge Porn and Mental Health: A Qualitative Analysis of the Mental Health Effects of Revenge Porn on Female Survivors" (2016) 12-1 Feminist Criminology 22; Clare McGlynn et al, "'It's Torture for the Soul': The Harms of Image-Based Sexual Abuse" (2021) 30:4 Social & Legal Studies 541.

Recommendations

1. Fast-track Option to Remove Intimate Images

One of the greatest concerns for those impacted by TFV is getting the harmful content swiftly removed from the internet before it replicates further.[4] This is particularly important for people who have had their intimate images shared without consent. The 2021 *Uniform Non-Consensual Disclosure of Intimate Images Act* (*Uniform Act*)[5] proposes a fast track option for those who simply want their intimate image taken down from the internet. In cases involving intimate images, it is quite simple to determine if something is an intimate image. A person will need to identify that the image is of them and that they did not consent to it being shared.[6] A fast-track option could be implemented without triggering serious freedom of expression concerns.

Accessing an order from the court may be critical to getting content removed. While CyberScan currently offers some support in helping victims remove images, many websites will not remove content from their sites without a court order. Providing an inexpensive, fast-track option for content that is clearly illegal would provide the remedy that most are calling for. This would be a good first step towards providing the remedies that would best match what those targeted by these harms are calling for.

It should be noted that as a formal legal procedure, even this fast track option may still cause barriers for some. To remove some of those barriers, accessible supports should be available through CyberScan in order to help people navigate this procedure and file the necessary documents for the fast-track option. Without additional supports, marginalized people without the resources to hire a lawyer to file these documents or assist them with the procedure, may be left without an accessible remedy. Further supports should be made available once a court order has been granted, such as assisting people with communicating those orders to websites or social media platforms in order to get the content removed or de-indexed. As will be discussed below, having a central government agency, such as CyberScan, that has regular communication with many of the websites and social media companies where these images are commonly posted can simplify and improve the practical effectiveness of take-down orders.

Recommendation:

We recommend that the *Act* be amended to include a fast-track option for those people seeking declaratory and injunctive relief with regards to intimate images.[7]

---

[4] Meghan Sali, "Intimate Images and Authors' Rights: Non-Consensual Disclosure and the Copyright Disconnect" (2022) 19 Can J L & Tech 333.
[5] Also see Emily Laidlaw & Hilary Young, "Creating a Revenge Porn Tort for Canada" (2020) Supreme Court Law Review.
[6] See pages 6-9 of the *Uniform Act* for more details on this subject.
[7] *Uniform Act,* s 4, p 6.

We recommend that CyberScan be mandated via regulation to provide supports to people in filing and implementing those orders.

2. Reverse Onus on Consent and Expectations of Privacy

Nova Scotia's *Act* was one of the first of its kind in Canada. Over time, other jurisdictions have begun introducing their own acts, many of which include a reverse onus on the defendant in cases of NCDII to prove that there was no reasonable expectation of privacy in the image and/or that they had consent to share the image.[8] In the case of consent, what this means is that when "an action is commenced, the intimate image is presumed to have been distributed without the consent of the person depicted and the defendant must establish that they had reasonable grounds to believe they had ongoing consent for distribution of that image."[9] Similarly, an intimate image should be presumed to have a reasonable expectation of privacy and the defendant must establish that there was not. Due to the inherently private nature of intimate images, it is reasonable for the courts to assume a person would not give consent to distribute those images and that there would be a reasonable expectation of privacy in the images.

Recommendation:

We recommend that the *Act* be amended to include a reverse onus on the defendant in cases of NCDII in regards to the reasonable expectation of privacy in the image and consent to distribute.

3. Automatic Anonymity for Targets of NCDII

Section 9 of the *Act* allows for a publication ban where intimate images have been distributed. Currently, this is granted upon request. Many targets of NDCII are reluctant to file court cases without being guaranteed anonymity as they are concerned that a public filing may bring more attention to the images. This is particularly true in smaller provinces and smaller communities, where issues of anonymity are much more difficult than in larger urban centres. A publication ban for plaintiffs in these cases should be automatic, as it is in the case for minors who have been cyberbullied, with an option for the person targeted by the NCDII to request the removal of the ban. An automatic publication ban in these cases would remove an unnecessary financial and procedural burden as most people involved in these types of cases would reasonably request a publication ban due to the inherent privacy interests in the images. In those rare circumstances where the applicant does not want a publication ban on the case, an option for removal of the ban should be available.

---

[8] For example *Intimate Images Protection Act*, SNL 2018; Bill 51, *The Privacy (Intimate Images – Additional Remedies)* Amendment Act, 2nd Sess, 29th Leg, Saskatchewan, 2021; Bill 69, *Intimate Images Unlawful Distribution Act*, 1st Sess, 60th Leg, New Brunswick, 2021.

[9] Pam Hrick, "Image-Based Abuse and Stalkerware in Intimate Partner Relationships: Towards an Effective and Victim-Centric Canadian Response" (2019) LLM Directed Research Project, New York University.

Recommendation:

We recommend that section 9 of the *Act* be amended so that a publication ban would automatically be implemented in cases involving the non-consensual distribution of intimate images, with an option for a request to remove the ban from the person targeted by the distribution.[10]

4. Include Altered Images and Nearly Nude Images as Intimate Images

In many jurisdictions, altered images have been included in the definition of intimate images.[11] New forms of technology have been developed that allow people to create realistic looking nude images of a specific person as well as sexual videos where it appears that someone is engaging in sexual acts they never actually engaged in.[12] Simple technology like Photoshop can create these realistic digitally altered images; however, in recent years artificial intelligence has been used to create "deepfake" videos where a person's face can be swapped into a pornography video. Women are the primary targets of this technology and almost all of these creations are made without consent of the women featured in them.[13] Due to their realism, these technologically generated images can have the same reputational repercussions and negatively impact a person's sexual expression and autonomy.[14] As such, altered images should be included in the definition of intimate images.

The *Uniform Act* recommends the inclusion of altered images as well as nearly nude images where there was a reasonable expectation of privacy in a nearly nude image. A definition of intimate images that includes nearly nude images would allow for the inclusion of clearly private and intimate images where a person is nearly nude but may not have their genitals or nipples directly exposed, but will avoid an over censoring of nearly nude images such as a woman wearing a bikini on a pubic beach.[15]

Recommendation:

We recommend that the definition of intimate images be amended to include altered images and nearly nude images.[16]

---

[10] *Uniform Act,* s 7, p 11.

[11] *Bill 69, Intimate Images Unlawful Distribution Act*, 1st Sess, 60th Leg, New Brunswick, 2021; *Australia Crimes Amendment (Intimate Images)* Act 2017 (New South Wales).

[12] Suzie Dunn, "Technology Facilitated Gender-Base Violence: An Overview" (2020) CIGI Supporting a Safer Internet Project Paper No. 1, online: <https://www.cigionline.org/publications/technology-facilitated-gender-based-violence-overview/>

[13] Henry Ajder, Giorgio Patrini, Francesco Cavalli & Laurence Cullen, "The State of Deepfakes- Landscape, Threats, and Impact" (2019) Deeptrace.

[14] Danielle K Citron & Robert Chesney, "Deep Fakes: A Looming Challenge for Privacy, Democracy, and National Security" (2019) 107 California Law Review 1753.

[15] *Uniform Act*, p 5.

[16] *Uniform Act*, p 3-5.

5. Consent to Distribution Should be Revocable

The *Act* should clarify that consent to the distribution of an image should be revocable. When relationships and circumstances change, a person's relationship to their intimate images will change along with them. As such, a person should be able to revoke the consent to share intimate images. When a person featured in the intimate images communicates to another person in possession of their intimate images that they no longer consent to them being distributed, that person must take every effort to remove and delete those intimate images. Following the communication of the revocation of consent, the defence of consent would no longer be applicable to a claim for distribution.

Recommendation:

We recommend that the *Act* be amended to allow for consent to be revoked.[17]

6. Public Figures' Intimate Images Should Generally not be of Public Interest

Section 7 of the *Act* includes a defence for the distribution of an intimate image without consent if the image in question is in the public interest. The limits of what is in the public interest[18] should be more precisely defined in this section. Many women in leadership roles have had their nude and sexualized images used to discredit them even though the images had nothing to do with their capacity to serve in a leadership position. In Nova Scotia, at least two female politicians have been targeted because of their intimate images. This happened to Robyn Ingraham, former Liberal candidate for Dartmouth South, whose old boudoir photos led to her being removed from running for the party, as well as the case of Lenore Zann, whose nude acting images were decontextualized and reposted on Twitter in an erroneous connection to her political career.[19]

The *Act* should include language that states that an intimate image is not in the public interest solely because the person is a public figure. While there may be some cases where a public figure's intimate images is of public interest, however, that must be assessed by the court on a case by case basis. An automatic publication ban should apply in cases where the public figure is a victim of NCDII that is not relevant to the public interest.

---

[17] *Uniform Act,* s 11, p 14.

[18] *Grant v Torsar,* 2009 SCC 61 at paras 102, 106, 107. In this case the definition of public interest was discussed: "How is 'public interest' in the subject matter established? First, and most fundamentally, the public interest is not synonymous with what interests the public. The public's appetite for information on a given subject — say, the private lives of well-known people — is not on its own sufficient to render an essentially private matter public for the purposes of defamation law. An individual's reasonable expectation of privacy must be respected in this determination. Conversely, the fact that much of the public would be less than riveted by a given subject matter does not remove the subject from the public interest. It is enough that some segment of the community would have a genuine interest in receiving information on the subject."

[19] Wayne MacKay , "Law as an Ally or Enemy in the War on Cyberbullying" (2015) 56 UNB Law J 3 at 46.

Recommendation:

We recommend that section 7 of the *Act* be amended to include specific language that states that a nude image is not in the public interest solely because the person is a public figure.[20]

7. Reconsider the Use of the Word "Cyberbullying"

The term "cyberbullying" evokes an image of children being cruel to each other on the internet, which limits the understanding of the breadth of what the *Act* actually covers. The term minimizes the severity of some of the behaviours covered in the *A*ct, as they are much more serious than bullying, which in itself is quite serious.[21] By using the term "cyberbullying", adults may not realize that they are also protected by this *Act*. A term such as "technology-facilitated violence, harassment, and abuse" (TFV) or "digital abuse" may be more appropriate.

Recommendation:

We recommend that "cyberbullying" be replaced with "technology-facilitated violence, harassment, and abuse" or "digital abuse".

8. Equality-focused Understanding of Freedom of Expression

One of the stated goals of the *Act* is to "uphold and protect the fundamental freedoms of thought, belief, opinion and expression, including freedom of the press and communication media." LEAF fully supports this goal and encourages the Nova Scotia government to take an equality-focused approach to freedom of expression in Canada.

In all deliberations about regulating content online, is important to recognize that Canadian constitutional law justifies imposing proportionate limits on freedom of expression in order to uphold and protect the rights to equality and freedom from discrimination, and also to give full effect to the core values underlying freedom of expression.[22]

Too often, discussions about problematic speech on the internet and freedom of expression are centred solely on the rights of the speaker of the harmful expression and whether their expression should be protected. These conversations often neglect to take into consideration how failing to regulate harmful and/or illegal speech significantly impacts the ability of others to speak freely. Research has shown time and time again that hateful, sexist, homophobic, and racist speech results in members of equality-deserving groups, including young people, women, and racialized groups, silencing themselves because they do not feel safe to express their thoughts and

[20] *Uniform Act,* s 10, p 13.

[21] Jane Bailey, ''Time to Unpack the Juggernaut? Reflections on the Canadian Federal Parliamentary Debates on 'Cyberbullying'" (2014) 37:2 Dal LJ 66.

[22] For a more fulsome discussion on this topic and the relevant case law to date, please review pages 176-192 of Deplatforming Misogyny.

opinions.[23] This silencing effect needs to be given proper weight when considering regulations to online expressive content. Without protecting equality-deserving groups from harmful and illegal speech, their freedom of expression is unfairly fettered.

Further, as noted by Cynthia Khoo, "the right to equality and freedom from discrimination are as fundamental and as protected by the Canadian *Charter of Rights and Freedoms* as is freedom of expression."[24] Thus, equality considerations should take an equal footing to freedom of expression in these conversations.

As Nova Scotia considers adjustments to this legislation and regulation, it must ensure that equality, freedom from discrimination, and freedom of expression are considered from this broad equality-focused perspective of freedom of expression. It must be understood that freedom of expression can be accompanied with duties and responsibilities and it is not synonymous with freedom from regulation.

Recommendation:

We recommend that the Nova Scotia government take an equality-focused approach when upholding and protecting fundamental freedoms of thought, belief, opinion and expression. This includes considering both the silencing impact harmful speech may have on those it is aimed at, as well as the right of a person to express that harmful speech.

9. Additional Supports for those Pursing Legal Action

As recently noted by Professor Emeritus Wayne MacKay,[25] when the original *CyberSafety Act* was struck down due to freedom of expression issues and the new *Act* was drafted, the pendulum may have swung too far in the other direction when it comes to the supports CyberScan can provide to people who contact them about pursing a legal solution. Many of the powers originally granted to CyberScan were removed when the Supreme Court of Nova Scotia found that the *CyberSafety Act* was unconstitutional for its overly broad definition of cyberbullying. This removed some of the effectiveness of CyberScan's ability to help the very people it was tasked to support. Filing the necessary legal paperwork is a complicated process that may seem out of reach for the average

[23] Cynthia Khoo, "Deplatforming Misogyny" (April 2021) at 177, online (pdf): Women's Legal Education and Action Fund https://www.leaf.ca/publication/deplatforming-misogyny/; Sharon Goulds et al "Free to Be Online" (Plan International, 2020); Azmina Dhrodia, "#Toxic Twitter: Violence and Abuse Against Women Online" (London, UK: Amnesty International, 2018); "Measuring the Prevalence of Online Violence Against Women" (2021) The Economist Intelligence Unit; "Methodology: Measuring the Prevalence of Online Violence against Women" (2021) The Economist Intelligence Unit; Rosel Kim & Cee Strauss, "Of Commitment and Precarity: Community-Based Approaches to Addressing Gender-Based Online Harm" in Anastasia Powell, Asher Flynn, & Lisa Sugiura, eds, *The Palgrave Handbook on Gendered Violence and Technology* (London: Palgrave Macmillan) 607-629.

[24] Cynthia Khoo, "Deplatforming Misogyny" (April 2021) at 177, online (pdf): Women's Legal Education and Action Fund < https://www.leaf.ca/publication/deplatforming-misogyny/>

[25] Portia Clark, "Province Seeks Feedback on Intimate Images and Cyber-protection Act" CBC Information Morning (10 January 2022), online: <https://www.cbc.ca/listen/live-radio/1-27-information-morning-ns/clip/15888096-province-seeks-feedback-intimate-images-cyber-protection-act>

person, especially young people. Without supports, the *Act* lacks effectiveness and remains inaccessible to those who need it most.[26]

In reviewing the current state of the *Act*, the province should reassess the powers granted to CyberScan and consider broadening them.

For example, it would be helpful if CyberScan had the ability to help investigate reports of TFV, digital abuse, and NCDII; provide practical support to those choosing to launch court actions, and assist those who have been granted a court order in getting content taken down. If CyberScan was tasked with supporting people who wish to get content taken down once they were granted a court order, it could work directly with individuals, websites, and social media platforms in getting content taken down. This would remove the burden from individuals who have been harmed by those online behaviours prohibited under the *Act*. This would prove particularly useful when it comes to communicating with social media companies whose content moderation systems can be difficult for the average person to navigate.

This model has proven to be successful in Australia where the Australian Government's eSafety Commissioner provides these types of supports.[27] The eSafety Commission has close relationships with social media platforms like Facebook, Instagram, and Twitter. As an individual user, these companies can be nearly impossible to get a hold of and it can be confusing to learn where and how to report problematic content, or where to send a court order to in order to have the content removed. Having a governmental body with direct contact with the companies can speed up the process in getting illegal content removed and can lift an unnecessary burden from individuals.

To date, there have been very few claims brought under the *Act.* As the rates of TFV, harassment, and NCDII are on the rise in Canada,[28] this suggests that the *Act* in its current form is not accessible enough to those it is meant to protect or it is not providing the remedies that people desire. The types of regulatory changes to CyberScan suggested above could increase the accessibility of legal remedies for those that desire and deserve them.

Recommendation:

We recommend that the *Act's* regulations be amended to allow CyberScan to provide more direct supports to those who wish to pursue a civil remedy and that CyberScan be provided with the resources to adequately support those seeking this type of assistance.[29]

---

[26] We recommend looking to British Columbia's Civil Resolution Tribunal as an example of how supports can be provided to people wanting to understand and bring forward a legal claim. Online: <https://civilresolutionbc.ca/>.

[27] Pam Hrick, The Potential of Centralized and Statutorily Empowered Bodies to Advance a Survivor-Centered Approach to Technology-Facilitated Violence Against Women (Bingley, UK: Emerald Publishing, 2021), online: <https://www.emerald.com/insight/publication/doi/10.1108/9781839828485> .

[28] Statistics Canada, "After five years of increases, police-reported crime in Canada was down in 2020, but incidents of hate crime increased sharply" (27 July 2021), Online: <https://www150.statcan.gc.ca/n1/daily-quotidien/210727/dq210727a-eng.htm>.

[29] Deleting Digital Harms, at p 21.

10. Technical, Emotional, Relationship-based, and Restorative Solutions

As stated by Professor Emeritus Wayne MacKay, "complex social problems usually require a multi-tiered response, including education, prevention strategies and other 'softer' responses, as well as the iron fist of the law."[30] CyberScan plays an important role in providing some of these softer, non-legal responses, as well as engaging in education and prevention strategies.

Alexa Dodge recently published a report, "Deleting Digital Harm: A Review of Nova Scotia's CyberScan Unit",[31] which reviewed CyberScan's current practices. In it, Dodge made multiple recommendations on how the organization could be improved. Her report demonstrated that many people who contacted CyberScan were not interested in a legal response if a technical, emotional, or relational response could resolve the issue.

As noted by Dodge:

> [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.[32]

Technological, emotional, relational, and restorative approaches are often the preferred method of resolution for the majority people involved in of these types of cases. Building on CyberScan's capacity to engage in this type of work would fulfil a significant need. These types of responses are less resource-intensive than pursing civil or criminal legal responses and can avoid putting additional pressures on the courts if non-legal solutions are available. They are also less resource intensive for those harmed and provide more accessible responses to those in need. This is particularly true for children, who may not view the justice system as a reasonable solution to their problems.[33]

For example, some people may need help figuring out how to report the content to a social media company. Many forms of TFV, digital abuse, and NCDII content are already prohibited on most major social media platforms. However, these companies' content moderation rules can be difficult to navigate for many people. Some people simply need help in reporting the content and the social media company may remove it if it violates their rules once it is reported. As such, it

---

[30] Wayne MacKay , "Law as an Ally or Enemy in the War on Cyberbullying" (2015) 56 UNB Law J 3.
[31] Alexa Dodge, "Deleting Digital Harms: A Review of Nova Scotia's CyberScan Unit" (2021) Dalhousie University, online: <https://www.vawlearningnetwork.ca/docs/CyberScan-Report.pdf>.
[32] *Ibid* at p 4.
[33] Jane Bailey & Valerie Steeves, "Defamation Law in the Age of the Internet: Young People's Perspectives" (2017) Law Commission of Ontario.

would be very helpful for CyberScan to provide support in assisting with takedown procedures. In more severe cases requiring immediate action, this process can be sped up if statutorily mandated bodies like CyberScan have regular contact with social media companies who they can contact when needed.[34] This can ensure swifter removal of harmful content that violates a social media companies own content moderation rules, without having to get the legal system involved at all.

CyberScan could improve its methods by focusing more on survivor-centric, trauma-informed, restorative justice models wherever possible. It should seek out expert advice on how to do this by seeking input and collaboration from those people impacted by these harmful online behaviours, the marginalized communities most impacted by these harms, and community based organizations with expertise in restorative and survivor-centric models, including anti-violence, Indigenous, Black Nova Scotian, 2SLGBTQQIA, disability, and anti-racism organizations, to name a few.

Recommendation:

We recommend that CyberScan build up its capacity to engage in survivor-centric, trauma informed, and restorative justice approaches.[35]

We recommend that CyberScan's mandate be revised to include a more central focus on technical, emotional and relationship-based approaches.

11. Better Public Awareness of CyberScan

CyberScan is an important resource for people harmed by TFV, digital abuse, and NCDII, however, it is not as well-known as it could be. For example, as noted in Dodge's report, CyberScan's website and promotional material could be improved to highlight the variety of legal information and non-legal services CyberScan provides to people harmed by TFV, digital abuse, and NCDII.

As TFV, digital abuse, and NCDII is on the rise, It is essential that the public becomes better aware of this service so they know how to access it when the time comes and what services CyberScan can provide. Adults and children alike should be familiar with CyberScan and be made aware that they can access those services. This includes informing schools, universities, libraries, community-services organizations, and other similar organizations about CyberScan so they can steer their students and clients to CyberScan when they need supports with these types of digital harms.

Importantly, CyberScan's policies should be updated to allow children to speak with CyberScan without parental/guardian permission. Often, children are reluctant to have adults (such as parents or teachers) involved when they are bullied or abused online. They may need to learn

[34] Pam Hrick, The Potential of Centralized and Statutorily Empowered Bodies to Advance a Survivor-Centered Approach to Technology-Facilitated Violence Against Women (Bingley, UK: Emerald Publishing, 2021), online: <https://www.emerald.com/insight/publication/doi/10.1108/9781839828485>.
[35] See Deleting Digital Harms, at p 12.

about what their options are and have someone validate that what is happening to them is wrong before deciding what to do and telling a trusted adult. Young people should be able to access this service without parental/guardian permission like they would with other child-centred services like the Kids Help Phone. Otherwise, we risk leaving children without the supports they deserve and leaving them at risk of continued digital abuse.

Recommendations:

We recommend that additional efforts be made to promote the services of CyberScan in a way that is understandable to the public, particularly to groups who are vulnerable to TFV, digital abuse, and NCDII.[36]

We recommend that promotional material about CyberScan include information about the services it provides to those seeking legal and non-legal solutions to harmful online behaviours captured under the *Act*.[37]

We recommend that young people be able to speak with CyberScan without parental/guardian permission.[38]

12. Education Focusing on Culture and Systemic Change

Two of the main goals of the *Act* are to "discourage, prevent and respond to the harms of non-consensual sharing of intimate images and cyberbullying" and to "help Nova Scotians respond to non-consensual sharing of intimate images and cyberbullying."

One of the best ways to prevent TFV, digital abuse, and NCDII is to change the norms around those issues through research and education.[39] Research is needed to fully understand what the issues are, what meaningful and accessible responses look like, and who is most affected by this harmful behavior. Education should focus on helping people understand what TFV, digital abuse, cyberbullying, and NCDII are; what help is available to those harmed by those actions, what people's rights are, and how to navigate difficult experiences online. This should include approaches that focus on consent, equality, anti-discrimination, and healthy relationships.[40] Similarly to sexual assault, NCDII suffers from sexist myths that victim blame those who have had their images shared without consent. Education could assist in dispelling those myths.

---

[36] See Deleting Digital Harms, at p 16.
[37] See Deleting Digital Harms, at p 24.
[38] See Deleting Digital Harms, at p 32.
[39] Anastasia Powell et al., "Image-based sexual abuse: An international study of victims and perpetrators. A Summary Report" (February 2020) at 12, online (pdf): RMIT University <https://researchmgt.monash.edu/ws/portalfiles/portal/319918063/ImageBasedSexualAbuseReport_170220_WEB_2.pdf>.
[40] See Deleting Digital Harms.

It is important to educate people about online safety planning, cybersecurity and privacy practices. However, the central educational goal out of CyberScan should be focused on changing people's perspectives around respectful and acceptable behaviour online broadly.

As recommended in *Deplatforming Misogyny*, educational materials should cover topics such as "technological literacy; the broader social context in which TFGBV is grounded; preventing TFGBV; challenging or refraining from victim-blaming; the lived experiences of those impacted by TFGBV; and providing a trauma-informed and victim/survivor-centred response in cases of TFGBV."[41]

Recommendation:

We recommend that CyberScan's research and education materials include:

a) broader social context of how systemic racism, sexism, colonialism, ableism, homophobia, transphobia, and other intersecting forces of marginalization contributes to TFV and digital abuse;
b) challenges to victim-blaming myths and stereotypes about TFV and digital abuse;
c) a focus on equality, healthy relationships, consent, and empathy;[42]
d) material on long-term change, community healing, and restorative justice;
e) trauma-informed and survivor-centric approaches to supporting those experiencing TFV and digital abuse; and
f) research on the trends and effects of TFV and digital abuse.

13. Providing Resources to Community Organizations

Although this review is focused on the *Act*. It is important to emphasize that only changing the law will not be sufficient to address this issue. One of the key places where supports, resources, and change are required is through front-line community organizations where people are already seeking community based supports. *Deplatforming Misogyny* notes the importance of funding frontline support workers and community-based organizations that have been working to end and support those experiencing TFGBV.[43] These community-based organizations possess the knowledge and community connections to effectively support the multifaceted needs of people experiencing TFV, digital abuse, and/or cyberbullying. These are the organizations that many of those targeted by harmful online behaviour are already seeking help, and they should be better resourced.

[41] Cynthia Khoo, *Deplatforming Misogyny* (April 2021) at 229, online (pdf): Women's Legal Education and Action Fund < https://www.leaf.ca/publication/deplatforming-misogyny/>.
[42] See Deleting Digital Harms at 49.
[43] Cynthia Khoo, *Deplatforming Misogyny* (April 2021) at 230, online (pdf): Women's Legal Education and Action Fund < https://www.leaf.ca/publication/deplatforming-misogyny/>

Recommendation:

We recommend that the educational mandate of CyberScan include providing resources to equality-focused community-based organizations that provide support to youth and adults, in order to ensure they are able to provide informed and well-resourced services to their clients experiencing TFV, digital abuse, or NCDII.

We recommend that additional government funding be provided for front-line organizations that are assisting people targeted by TFV, digital abuse, or NCDII.

Conclusion

This submission provides several recommendations for changes to the *Act* including adding a fast-track option for individuals who have had their intimate images distributed without consent, a reverse onus for consent and the reasonable expectation of privacy in cases of NDCII, an automatic publication ban in cases of NCDII, a definition of intimate images that includes nearly nude images and altered images, and a more clearly defined understanding of what is in the public interest. However, some of the most important recommendations are those involving policy and regulatory changes. Many of these recommendations can be implemented through changing the regulations associated with the *Act.*

We want to emphasize that while we recognize that civil legal action will be useful and necessary to many people harmed by those behaviours prohibited by the *Act,* research shows that what most people want is direct supports that can help with getting content taken down quickly. In some cases, this may require a court order, but in many, non-legal solutions will be the most desirable. Services by CyberScan and other frontline organizations that provide supports to the people affected and help mend individual relationships and communities are key. Beyond these immediate supports, regulations, resources, and policy changes that focus on research and education will provide the longer term solutions needed to truly end these harmful behaviours. Nova Scotia should continue building on its a multi-faceted approach through additional law reform, regulatory change, front-line service supports, research, and education in order to meaningfully address this problem.

Appendix

1. We recommend that the *Act* be amended to include a fast-track option for those people seeking declaratory and injunctive relief with regards to intimate images.

2. We recommend that CyberScan be mandated via regulation to provide supports to people in filing and implementing those orders.

3. We recommend that the *Act* be amended to include a reverse onus on the defendant in cases of NCDII in regards to the reasonable expectation of privacy in the image and consent to distribute.

4. We recommend that section 9 of the *Act* be amended so that a publication ban would automatically be implemented in cases involving the non-consensual distribution of intimate images, with an option for a request to remove the ban from the person targeted by the distribution.

5. We recommend that the definition of intimate images be amended to include altered images and nearly nude images.

6. We recommend that the *Act* be amended to allow for consent to be revoked.

7. We recommend that section 7 of the *Act* be amended to include specific language that states that a nude image is not in the public interest solely because the person is a public figure.

8. We recommend that "cyberbullying" be replaced with "technology-facilitated violence, harassment, and abuse" or "digital abuse".

9. We recommend that the Nova Scotia government take an equality-focused approach when upholding and protecting fundamental freedoms of thought, belief, opinion and expression. This includes considering both the silencing impact harmful speech may have on those it is aimed at, as well as the right of a person to express that harmful speech.

10. We recommend that the *Act's* regulations be amended to allow CyberScan to provide more direct supports to those who wish to pursue a civil remedy and that CyberScan be provided with the resources to adequately support those seeking this type of assistance.

11. We recommend that CyberScan build up its capacity to engage in survivor-centric, trauma informed, and restorative justice approaches.

12. We recommend that CyberScan's mandate be revised to include a more central focus on technical, emotional and relationship-based approaches.

13. We recommend that additional efforts be made to promote the services of CyberScan in a way that is understandable to the public, particularly to groups who are vulnerable to TFV, digital abuse, and NCDII.

14. We recommend that promotional material about CyberScan include information about the services it provides to those seeking legal and non-legal solutions to harmful online behaviours captured under the *Act*.

15. We recommend that young people be able to speak with CyberScan without parental/guardian permission.

16. We recommend that CyberScan's research and education materials include:

    a. broader social context of how systemic racism, sexism, colonialism, ableism, homophobia, transphobia, and other intersecting forces of marginalization contributes to TFV and digital abuse;
    b. challenges to victim-blaming myths and stereotypes about TFV and digital abuse;
    c. a focus on equality, healthy relationships, consent, and empathy;
    d. material on long-term change, community healing, and restorative justice;
    e. trauma-informed and survivor-centric approaches to supporting those experiencing TFV and digital abuse; and
    f. research on the trends and effects of TFV and digital abuse.

17. We recommend that the educational mandate of CyberScan include providing resources to equality-focused community-based organizations that provide support to youth and adults, in order to ensure they are able to provide informed and well-resourced services to their clients experiencing TFV, digital abuse, or NCDII.

18. We recommend that additional government funding be provided for front-line organizations that are assisting people targeted by TFV, digital abuse, or NCDII.