

SUCCESSES, CHALLENGES, & VISIONS FOR THE FUTURE:

INSIGHTS FROM THE MARCH 2026 “DIGITAL SAFETY IN CANADA” WORKSHOP

Participants from DIY: Digital Safety,
CyberSCAN, the Canadian Centre for Child Protection,
and British Columbia's Civil Resolution Tribunal



BACKGROUND

In March of 2026, the **DIY: Digital Safety research group**, in collaboration with the Dalhousie University's Schulich School of Law's **Law and Technology Institute**, met for a two-day workshop that brought Canadian digital safety workers and researchers together in Halifax, Nova Scotia to discuss the state of digital safety and responses to technology-facilitated violence in Canada. Participants in the workshop included representatives from organizations working directly to prevent and respond to technology-facilitated violence in Canada, including Nova Scotia's CyberSCAN unit, the Canadian Centre for Child Protection (C3P), and British Columbia's Civil Resolution Tribunal (CRT). The workshop aimed to bring together a network of knowledge and resource sharing to increase digital safety for all Canadians. This report outlines key takeaways from this workshop, including some of the current successes in Canada's response to digital harms, some of the continued challenges in Canada's response, and a vision for the future of digital safety in Canada.

ABOUT THE DIGITAL SAFETY ORGANIZATIONS INVOLVED

DIY: Digital Safety: A team of leading Canadian scholars on technology-facilitated violence, including Dr. Kaitlynn Mendes, Dr. Alexa Dodge, Dr. Christopher Dietzel, and Professor Suzie Dunn. The DIY team has significant experience mobilizing knowledge through academic and non-academic communities, including creating numerous public reports, fact sheets, and infographics on digital safety issues and supports. Their publications are based on qualitative, quantitative, and doctrinal research about Canadians' experiences with technology-facilitated sexual violence and other online harms.

Canadian Centre for Child Protection (C3P): The Canadian Centre for Child Protection is a national charity dedicated to the personal safety of all children. Their goal is to reduce the sexual abuse and exploitation of children. Some of C3P's many initiatives that are relevant to the digital safety mandate include their tipline for reporting child sexual abuse material (Cybertip.ca), their child sexual abuse material removal tool (Project Arachnid), and their support service for those under 18 who have had or are being threatened with the distribution of their intimate image without consent (Need Help Now). They are also mandated to provide supports for adults in Manitoba who have been victimized by the non-consensual distribution of intimate images.

CyberSCAN: Nova Scotia's CyberSCAN unit can help support Nova Scotians of any age who are experiencing cyberbullying or the non-consensual distribution of their intimate images. Staff support victims through information about their legal and non-legal support options and can help report and remove content shared without consent online.

Civil Resolution Tribunal, Intimate Images: Under British Columbia's **Intimate Images Protection Act**, the Civil Resolution Tribunal (CRT) allows those who have had their intimate images shared or threatened to be shared without consent to make a claim for an intimate image protection order. This fast-track legal option can order someone to delete the image or stop them from sharing or threatening to share it. Claims for damages and administrative penalties can also be made. British Columbia also has an **Intimate Image Protection Service** that provides emotional supports, resources, and legal information to survivors of non-consensual intimate image distribution.

CURRENT SUCCESSES

Relatively rapid response and effective takedown models for victims under 18 and for adults in some jurisdictions (e.g. Nova Scotia and British Columbia)

- Nova Scotia's CyberSCAN unit has reported relatively high success rates in removing non-consensually distributed content of both their adult and under 18 clients, including non-consensually distributed intimate images and other forms of non-consensual content. Clients appreciate being able to speak with a caring and supportive person rather than simply accessing online supports.
- British Columbia's CRT tribunal members can quickly issue a protection order for applicants whose intimate images have been shared or threatened to be shared. This includes orders to delete, destroy, de-index, and refrain from sharing intimate images without consent. Protection order claims can be resolved even where the applicant chooses not to name a respondent, balancing speed and survivor autonomy. Applicants can also be awarded up to \$75,000 in damages. If someone has failed to comply with a Protection Order, the applicant can apply to the CRT for an administrative penalty, which is like a fine payable to government. The CRT team is well trained on the law and trauma-informed practices.
- C3P is able to respond to cases involving minors across Canada, while their mandate for adults is limited to cases connected to Manitoba. They report a high success rate in removing child sexual abuse material (CSAM) and other content harmful to children, with particular success on most major platforms. Using the Project Arachnid model, they issue thousands of takedown notices to online services each day, leveraging cryptographic and perceptual hash-matching technologies (such as PhotoDNA) to identify and

seek the removal of harmful or illegal imagery. C3P is a trusted organization around the world, thereby supporting digital safety in Canada and internationally.

PROMISING LEGAL AND POLICY MECHANISMS

- Well-resourced and long-standing organizations, such as C3P, maintain a wide breadth of specialists including legal, research, technical, and front-line staff. These organizations are well equipped to understand existing trends in technology-facilitated harms and effective responses to them. Their Canadian based research outputs and specialized institutional knowledge help inform legal professionals, government and other child-serving stakeholders.
- CyberSCAN finds copyright law to be a useful tool for compelling platform action.
- Mandatory reporting frameworks for online services and the technology industry in Canada and the U.S. results in the reporting/flagging of confirmed or suspected child sexual exploitation and abuse which can lead to both law enforcement action against offending users and removal of the content itself.
- Growing cooperation among provincial and federal bodies, including trauma-informed and specialized training for staff, is contributing to positive outcomes.
- C3P maintains and develops a repository of victim impact statements linked to victims of "known CSAM" which can be filed under certain circumstances during sentencing for CSAM offenders.

SIMPLIFIED VICTIM PATHWAYS

- Accessible online and phone-based support services provide much-needed emotional, technical, and legal supports for some categories of victims in Canada (e.g. Nova Scotians through CyberSCAN and young people under 18 across Canada through C3P's various services – including [Cybertip.ca](#) and [NeedHelpNow.ca](#)).
- Fast-track legal options where victims can report their experiences of harm without the need for a lawyer (e.g. those available to British Columbians through the CRT) are much more accessible and expedient than traditional criminal or civil interventions.

WHAT'S NOT WORKING

STRUCTURAL & RESOURCE GAPS

- While CyberSCAN, C3P, and the CRT each respond to adult cases of non-consensual intimate images distribution in their provinces (and cyberbullying in the case of CyberSCAN), most Canadian provinces do not have these kinds of legal, technological, or emotional support services for adult victims of technology-facilitated violence. This leaves significant gaps for adult victims across provinces and territories without these supports.
- Existing organizations could benefit from additional resources and increased staffing to address the large scale and increasing reports of technology-facilitated harms in their respective provinces. For example, CyberSCAN has a single full-time staff person managing reports made from across the province to that organization. C3P also faces understaffing and resource limitations, particularly as the number of reports of online child sexual exploitation and CSAM grows with every passing year. The rate at which

C3P's Project Arachnid discovers CSAM on the internet outpaces its ability to review and classify the content, leading to a backlog of images and videos requiring manual review.

- There is a need for a coordinated Canada-wide response for nonconsensual intimate images of adults. This could include a centralized process for trusted flaggers and judges to easily register an image as a non-consensually distributed intimate image (NCDII) and trigger enforcement efforts for removal and the generation of digital hashes, which may then be used by online services to block the re-upload and further distribution of these images (similar to the technology used widely by the tech industry and groups like C3P to detect and block CSAM).
- There is a need for organizations that address a wider breadth of online harms to support all the needs of victims of technology-facilitated violence.

LEGISLATIVE AND ENFORCEMENT BARRIERS

- There is a lack of legal consistency across Canada, which causes confusion for victims and provides inconsistent response depending on the province.
 - Civil legislation addressing intimate images differs from province to province.
 - Only three provinces have government supported bodies that provide supports to victims.
 - Nova Scotia is the only province that also includes other forms of technology-facilitated harms (what it calls cyberbullying) in its legislation.
- Canada failed to pass Bill C-63 ("Online Harms Bill"), resulting in major legislative and support gaps across the country. There is a need for federal platform regulation that would provide a

duty to mitigate harms. A renewed effort under Bill C-34 (“Safe Social Media Act”) is underway, and includes provisions for the blocking of CSAM and NCDII in Canada within 24 hours when flagged.

- Companies face few consequences for non-compliance, and Canadian enforcement often stops short of holding large global tech entities accountable.
- Current supports are piecemeal and geographically specific. Many digital harms are not limited by geographic borders, which requires cooperation and coordination across jurisdictions and a national strategy for prevention and response.

AWARENESS AND ACCESSIBILITY

- Public understanding of available supports remains low, even in provinces with support services available. This issue is amplified by the fragmented landscape of agencies across Canada.
- Barriers include challenges in educating young people about technology-facilitated violence in schools in ways that are victim centred and youth-rights-focused.
- Training for legal actors, frontline victim services, and other supportive roles remains inconsistent nationwide. Frontline anti-violence organizations (e.g. domestic violence, gender-based violence, and at-risk youth organizations) report that their clients are experiencing these harms but that they often lack the training and resources to adequately support their clients.
- There is a dearth of Canadian research on effective responses to technology-facilitated violence.

VISIONS FOR THE FUTURE

LAW AND POLICY DEVELOPMENT

- Strengthen and harmonize laws about non-consensual distribution of intimate images across provinces. Every province should have legislation on the books that includes statutorily protected bodies that provide well-resourced supports to victims and produces research outputs based on their expertise.
- The federal government should establish laws that regulate online service providers.
- The federal government should create a body that provides supports to victims across Canada and coordinates with provincial bodies to provide stable funding to organizations working on the frontline of these issues.
- Create free, specialized legal advice and trauma-informed representation for victims of technology-facilitated violence (similar to the independent legal advice that is available to victims of sexual assault in some provinces).
- Develop judicial and bar specializations in digital harm and online abuse.
- Recognize doxing and privacy breaches as prosecutable harms.

NATIONAL COORDINATION AND OVERSIGHT

- Participants called for a national digital safety body – similar to Australia’s eSafety Commissioner – with provincial offices and consistent funding. This agency should have:
 - Regulatory powers to enforce a duty of care on online service providers.
 - 24-hour support resources available for citizens, including technological support (e.g. escalation and expedient reporting/removal of harmful/private content with

- non-compliant online services), legal/ support information, and crisis support.
- Provincial outreach partners to provide in-person accompaniment and ongoing case support.
- Research and public engagement teams that provide evidence-based research and knowledge mobilization.

- Develop a better understanding of why people choose various pathways to support and why those supports did or did not provide them with the help and/or remedy they desired.

IN SUMMARY:

Canada's digital safety ecosystem is making progress through localized expertise, compassionate processes, and trusted cross-sector partnerships. Yet, without a national coordinating body, modernized legislation, and scaled technological capacity, responses remain fragmented and under-resourced. A future-ready digital safety model will require unified governance, resourced agencies, rapid removal mechanisms, and a globally aware approach to online harms.

TECHNOLOGY AND GLOBAL ACCOUNTABILITY

- Implement standardized, transparent use of perceptual hashing and reporting mechanisms across platforms.
- Incorporate international cooperation about best practices among organizations providing research and responses to digital harms, recognizing that most content, perpetrators, and hosting sites lie outside Canada's jurisdiction.
- Support investigative journalism and civil society watchdogs who can put public pressure on non-compliant online service providers.

RESEARCH AND KNOWLEDGE BUILDING

- Conduct national mapping of NCDII and CSAM, and other technology-facilitated violence experiences, cases, and responses, including:
 - Success rates, process drop-out rates, and timeliness of takedowns among organizations providing supports and through the traditional legal system.
 - Comparative analysis of provincial laws and tribunal practices.
 - Evaluation of adult NCDII case law and enforcement outcomes.
 - Develop easy public "cheat sheets" outlining each platform's takedown processes.