sh!ft

THE PROJECT TO END DOMESTIC VIOLENCE

PROMOTING TECHNOLOGICAL SAFETY AND INCLUSION FOR PREVENTING DOMESTIC AND SEXUAL VIOLENCE

2022

UNIVERSITY OF CALGARY
FACULTY OF SOCIAL WORK

Authors
Anya Litviniuc
Lana Wells

Acknowledgement
Shift gratefully acknowledges the Max Bell Foundation for supporting this research project. We would like to thank Kim Nagan for her editorial support and the following experts that took the time to review an earlier version of the paper: Jane Bailey, Raine Liliefeldt, and Dr. Alina Turner. We would also like to thank the APPF Foundation Document Review Working Group Members for their feedback on the paper:

Amber Niemeier, YW Edmonton
Andrea Silverstone, IMPACT
Carrie McManus, IMPACT
Chris Johnson, Sanare Centre
Deb Tomlinson, Association of Alberta Sexual Assault Services
Diana Lowe, Reforming the Family Justice System
Giri Puligandla, Canadian Mental Health Association Edmonton
Jassim Al-Mosawi, CDVC/Mosaic Primary Care Network
Julie Peacock, Ministry of Community and Social Services
Krysta Halfe. Native Counselling Services of Alberta
Lindsay Whittaker, Ministry of Community and Social Services
Lisa Watson, Odyssey House
Lubna Zaeem, Islamic Family and Social Services Association

Suggested Citation
Litviniuc, A., & Wells, L. (2022). *Promoting technological safety and inclusion for preventing domestic and sexual violence.* Calgary, AB: The University of Calgary, Shift: The Project to End Domestic Violence.

Acknowledging Indigenous Territory and Peoples
Shift wants to acknowledge that our team members live across Turtle Island in what is today known as Canada. We acknowledge that the places we call home have deep ties to the Indigenous Peoples that have stewarded this land since time immemorial. We also acknowledge that colonial actors and institutions perpetually deny Indigenous Peoples their rights to self-determination and sovereignty and these institutions must be challenged and changed. Shift is committed to the advancement of the United Nations Declaration on the Rights of Indigenous Peoples and the Calls to Action of the Truth and Reconciliation Commission.

Contact
Lana Wells, Brenda Strafford Chair in the Prevention of Domestic Violence
Faculty of Social Work, University of Calgary
2500 University Drive NW, Calgary, AB, Canada T2N 1N4
Phone: 403-220-6484 Email: lmwells@ucalgary.ca

sh!ft
THE PROJECT TO END DOMESTIC VIOLENCE

TABLE OF CONTENTS

1.0 Introduction

The purpose of this report is to inform the design of the Alberta Primary Prevention Framework (APPF), whose goal is to help the Government of Alberta and the IMPACT collective to identify strategies and actions that are focused on upstream primary prevention efforts to stop domestic and sexual violence before it starts.

Primary prevention approaches focus on preventing initial perpetration and victimization of domestic and sexual violence by targeting the structural and cultural conditions that produce and reinforce violence.[1]

This definition means that we need to target the root causes and drivers of domestic and sexual violence. The **root causes** of domestic and sexual violence are **four systems of oppression**, specifically, heteronormative patriarchy, capitalism, white supremacy, and colonialism.[2]

Heteronormative patriarchy is a social system in which, on average, heterosexual men have the most power, privilege, and control in political, economic, cultural, and social roles.[3]

Capitalism is a socio-economic system focused on wealth accumulation and profit, which reinforces inequalities, competition, and exploitation of people and the environment.[4]

White supremacy is a social system in which white people overwhelmingly control power and material resources due to norms and behaviours of white superiority and entitlement, which lead to white dominance across institutions and social settings.[5]

Colonialism is a socio-economic system that maintains political and economic control over a marginalized social group within one's nation, or over other nations.[6]

These four systems of oppression normalize dominant groups' privilege and equity-deserving groups' oppression in norms, narratives, structures, systems, institutions, and interactions. This creates opportunities for perpetrators to use violence against equity-deserving groups by exploiting inequalities in status, power, and resources. While largely abstract, these systems of oppression manifest themselves in our structures, systems, institutions, and interactions as **drivers of domestic and sexual violence**. The drivers include **the normalization of violence and inequality,** and **gender and social inequalities**. These drivers make violence and inequality seem a natural part of social life and reinforce the domination of privileged groups, such as white heterosexual men, and the marginalization of women, equity-deserving groups, and Indigenous Peoples, all of which creates cultural and structural opportunities for domestic and sexual violence.

The drivers of violence show up in all areas of life, including in technological and digital domains. First,

the introduction of technology may increase inequalities. For example, over half of the increasing wage gap in recent decades appears to stem from technology, as employers pay workers less and spend more on technology.[7] This tendency results in employers creating a landscape of low-paying jobs that require limited skills.[8] As a result of growing poverty among low-skilled workers, domestic and sexual violence may increase.[9] Additionally, access to technology and technological capacity may increase inequalities, as the so-called "digital divide" reinforces the privilege of groups that have access to technology and technologically facilitated opportunities, marginalizing those who do not, for example, low-income individuals and residents of rural and remote communities. This results in the "inequality loop," with digital and social exclusion of equity-deserving groups reinforcing one another.[10]

Second, there are still striking gender and social inequalities in the technology industry. For example, in the USA, between 2018 and 2020, the number of female employees in the technology industry increased by just 2.9%, reaching 32% overall, and women's salaries in 2020 were still 2.5% lower than men's salaries.[11] This gender inequality in both employee make-up and pay makes technology industry rife with sexual harassment. In 2020, a survey of technology company founders found that 44% of women overall, 47% of women of colour, and 65% of 2SLGBTQIA+ individuals reported persistent sexual harassment.[12] Additionally, gender and social inequalities in the tech sector contribute to much of technology being either gender blind, inaccessible, and age-unfriendly or outright harmful for women and equity-deserving groups,[13] creating opportunities for domestic or sexual violence perpetrators to inflict additional damage through technology.

Third, digital spaces have become places of discrimination, exclusion, and radicalization, where perpetrators reinforce the marginalization of women and equity-deserving groups through sexual violence and create networks of abusers. One example of such a network is the "manosphere", a group of online men's communities with misogynist beliefs and practices oppose women's equality and empowerment.[14]

Finally, this topic is of major importance since the COVID-19 pandemic has increased both our reliance on technology and its potential to be misused for violence and abuse. On the one hand, technology has helped people work from home, remain connected with family and friends, and benefit from online counselling and telemedicine. Despite these positives impacts, early in the pandemic the impacts of inequitable access to technology or the Internet became very clear, with some people being prevented from having their basic needs met when most of the interactions moved online. For those living in risky situations or for equity-deserving groups technology also posed additional challenges. For example, abusers had more control over survivors' access to technology to increase their isolation and limit help-seeking.[15] Additionally, perpetrators invented new forms of technology-facilitated violence such as Zoom bombing, exposing women, especially female activists, to sexually explicit materials during videoconferencing.[16]

We can contribute to preventing domestic and sexual violence by addressing how the drivers of domestic and sexual violence show up in technological and digital domains and by promoting

technological safety and inclusion.* This can be achieved by ensuring technology is used to promote people's wellbeing and empowerment, especially among equity-deserving groups; by promoting equality and non-violence in the technology industry; and by making technology and digital spaces safe and inclusive.

In this report, we make a range of high-level recommendations, many of which focus specifically on preventing technology-facilitated violence, as research suggests this is a form of violence that is becoming more prevalent.[17]

> Technology-facilitated violence is any violence that is committed, assisted, or aggravated in part or fully by the use of the Internet or communication technologies, including social media platforms, email, forums, websites, messaging platforms, smartphones, etc.[18]

We offer the most promising legislation and policy guidance for technological safety and inclusion based on violence prevention and gender equality plans from Western countries with the most advanced violence prevention policies.† Additionally, we provide recommendations for preventing technology-facilitated violence based on research and recommendations by Canadian policy actors.‡ As we continue to depend on technology for many of our needs and interactions, it is crucial to build on the current momentum introduced by the federal government through its information and communication sector reforms.[19] Furthermore, we need to implement comprehensive evidence-based and evidence-informed preventative legislation and policies to provide equitable access to technology and ensure technological and digital safety and inclusion for all. The federal and provincial governments must spearhead these efforts because the constantly developing technology field requires their regulation and authority to negotiate controls with producers and service providers on local, provincial, national, and international levels. However, technological inclusion and safety also require a change in norms, culture, systems, and institutional capacity. Therefore, the anti-violence sector can also play a prominent role in leveraging technology for preventing domestic and sexual violence.

In the remainder of this report, we make a case for focusing on technological and digital inclusion and safety for preventing domestic and sexual violence; outline the types of technology-facilitated violence; and provide legislation and policy recommendations for the federal and provincial governments and the anti-violence sector in Alberta to stop violence before it starts.

---

* We use the term "technological safety and inclusion" to cover all technologically-facilitated interactions and digital spaces as well as the technology industry.

† The plans come from Australia, Canada, Denmark, Finland, New Zealand, Norway, and Sweden.

‡ For more information on our methodology, please see Appendix 1.

2.0 Rationale for ensuring technological and digital inclusion and safety to prevent domestic and sexual violence

The time is now for governments and the anti-violence sector to address technological and digital inclusion and safety for the following reasons:

1. **The COVID-19 pandemic has highlighted the inequities in access to technology and greatly increased the use and misuse of technology.**

The COVID-19 pandemic has made the Internet and technology indispensable. Since the onset of the pandemic, many areas of work, study, personal communication, and activities have moved online or become technologically mediated. Research shows that early in the pandemic, 75% of Canadians started using the Internet more often than before, and almost half used the Internet for a new digital activity for the first time.[20] At the same time, the pandemic has also highlighted inequalities in access to the Internet and technology. Anti-violence sector service providers have emphasized that some survivors of violence could not use professional services since they had no access to the Internet, computers, phones, or phone credit.[21]

As technology use has surged, rates of technology-facilitated violence have also increased. Canadian statistics show that incidents of non-consensual distribution of intimate images have increased by 10%, indecent or harassing communications by 9%, criminal harassment by 4%, and uttering threats by 3%.[22] Online victimization of children has also risen. For example, production or distribution of child pornography has risen by 27%, possessing or accessing child pornography by 19%, and luring a child through a computer by 15%.[23]

2. **Technology and digital platforms are often used to commit gender-based violence**.

Our advertising-driven business models prioritize profit over safety, especially equity-deserving groups' safety, and favours explicit sensationalized content, which often normalizes and glorifies violence.[24] For example, a Wall Street Journal study revealed that Facebook exempted its high-profile users from some control measures and allowed them to post material that included harassment and incitement to violence, which would typically lead to sanctions.[25] Furthermore, the management of the information and communication technology sector lacks diversity,[26] which impacts technology design and increases risks of its misuse against girls, women, and equity-deserving populations. As a result, even mainstream digital platforms routinely condone and perpetuate technology-facilitated violence, misogyny, racism, colonialism, homophobia, biphobia, transphobia, ableism, and other forms of discrimination. For example:[27]

- Facebook has kept flagged pages glorifying intimate-partner violence but has removed images of women breastfeeding.
- Twitter has suspended users targeted by online abuse but has frequently allowed abusive users to maintain their accounts.
- YouTube's recommendation algorithms have facilitated right-wing radicalization through its

platform.
- Google Search has provided racist, sexually objectifying images of Black girls and women as its top-ranked search results.

"When there is any type of digital violence, it's often against women and people of colour, and when you have men who are creating these technologies at these start-ups…they don't often perceive or foresee that type of violence."

Takara Small, Host and Producer of The Globe and Mail podcast "I'll Go First" and Founder of VentureKids Canada[28]

Additionally, there are purpose-built platforms that exist exclusively to promote technology-facilitated violence (e.g., platforms dedicated to sharing non-consensually distributed intimate images.) It is important to note that such harms are not limited to the digital realm, as technology-facilitated violence often transforms into face-to-face violence.[29] For example, joining an online community of misogynists or trolling women anonymously can lead to offline violence and heighten the risks that consumers of online violent content will enact it in real life.[30] We need look no further than the 2018 Toronto van attack perpetrator who spent hours on incel forums where he was radicalized.[31]

3. **Technology-facilitated violence is very hard to stop once perpetrated and its impacts are highly traumatic.**

The Internet and technology are convenient tools for inflicting violence. Victims can be abused through multiple means (e.g., on several digital platforms), in numerous ways (e.g., trolling or sharing non-consensual intimate images), in all locations, and at all times, with violence taking place in front of multiple social circles, and often strangers.[32] Thus, some forms of technology-facilitated violence have an extremely large audience, often far beyond the initially intended one, and even involve unsuspecting bystanders. Furthermore, the Internet and technology are iterative and permanent. Once shared, the material can be saved on other devices by intended and unintended recipients, disseminated across borders, and reproduced and changed with no control and slim chances of complete and permanent removal.[33] Finally, technology-facilitated violence can be particularly vicious and cruel since it may feel impersonal to perpetrators and less serious than face-to-face violence to bystanders, who may be less likely to intervene.

The impact of technology-facilitated violence is traumatizing and disruptive for victims. Some of its consequences include:[34]
- **Psychological impacts:** sadness, shame, trust and self-confidence issues, stress, anxiety, depression, fear, panic attacks, PTSD, and suicide.
- **Health impacts:** outcomes related to stress such as diabetes, cardiovascular disease, and worsening of pre-existing chronic conditions.

- **Social effects:** compromised sense of security, social withdrawal, isolation, compromised productivity at work, loss of income, and loss of reputation.[35]
- **Societal effects:** increased needs for and costs of health care, judicial, and social services; violation of free expression and other human rights;[36] perpetuation of misogyny and other forms of oppression; continued objectification and subordination of girls, women, and equity-deserving populations and their isolation in the digital and "real" world.[37]

4. **Technological exclusion and technology-facilitated violence further entrench social inequities and offset social progress.**

"Technology replicates systematic inequalities."

Nasma Ahmed, Director of the Digital Justice Lab[38]

Women, girls, equity-deserving populations, and people at the intersection of multiple forms of oppression are disproportionately impacted by technological exclusion and technology-facilitated violence, particularly in its sexualized form.[39] For example, women living with disabilities and using assistive devices and technology for communication are at greater risk as perpetrators may hack their devices, disrupt their access to supports, and exploit their dependence on others with greater ease.[40] Black, Indigenous, and Muslim women, and members of 2SLGBTQIA+ communities experience higher rates of online hate and harassment than other groups.[41]

5. **Government investment in ensuring access to the information and communication technology (ICT) sector is not always sufficient and is, therefore, exclusionary.**

Internet and technology access is an urgent issue to address because it is highly unequal for various social groups. For example, compared to almost 90% of urban Canada, only 53% of rural communities have access to unlimited broadband,[42] and compared with 98% of Canada's highest income households, only 59% of lowest income homes have Internet access.[43] Access to technological devices is also highly unequal. A Calgary-area survey revealed that only 47% of respondents had sufficient access to tablets and computers.[44] Despite federal government broadband investment, it has mostly resulted in unevenly distributed patchy networks.[45] Targeted investment in improving access to technological devices for people at risk has also been limited. Some Internet service providers have waived overage and data caps, have not disconnected accounts for non-payment, and have donated devices and service plans to populations most at-risk of digital exclusion; however, these measures have been temporary and have covered only a part of the population.[46]

6. **Government regulation of the ICT sector is lacking.**

As a result of quick advances in technology and the free market economy, there is limited legislation and policy to control the ICT sector. Regulations often lag behind technological innovations. In Canada, much of the Internet and communications legislation is regulated by the federal

government[47] and there are significant gaps when it comes to technology-facilitated violence. For example:

- Most **legislation and polices are reactive rather than preventative** and fail to take into account the **impact of oppression on equity-deserving groups**, who are most affected by technological exclusion and violence.
- There are **no specific forms of legal liability for many issues** (e.g., digital platforms hosting technology-facilitated violence), making it hard to force digital platforms to perform due diligence.[48] Furthermore, existing applicable laws are often not invoked against digital platforms.
- Many types of technology-facilitated violence fall through the cracks of the existing legislation (e.g., the current legislation against the distribution of non-consensual images does not cover deepnudes[§] and sexual deepfakes[**]),[49,50] which **fails to deter perpetrators** from committing such acts.
- The application of general laws of the Criminal Code sometimes results in decisions that fail survivors and reinforce **the myth that technology-facilitated violence is less harmful than physical violence.** For example, law enforcement and justice agents have a limited understanding of digital forensic evidence and limited skills for collecting and evaluating it,[51] or the impacts of technology-facilitated violence are considered not serious enough to justify criminal convictions.
- While existing legislation and policy offer adequate protection from online child sexual exploitation,[52] the **safety of older adolescents, youth, and other equity-deserving groups is not prioritized** in how the laws are applied.

7. The anti-violence sector has limited expertise in technology-facilitated violence.

Organizations in the anti-violence movement are still learning how to identify and mitigate the risks of technology for facilitating domestic and sexual violence.[53] Understanding many of the risks requires specialized knowledge that is not readily available in the sector, especially because there is limited funding and resources are already stretched.

For all these reasons it is essential for the government and the anti-violence sector to address technological exclusion and technology-facilitated violence, focusing on the rights of and impacts of oppression on women and equity-deserving groups.

[§] A software application that uses neural networks to remove clothing from the images of women, making them look realistically nude.[49]

[**] Realistic-looking video pornography that "utilizes artificial intelligence to depict sexually explicit acts involving people who didn't actually participate in those acts".[50]

3.0 Types of technology-facilitated violence

Technology-facilitated violence can be a stand-alone form of violence, committed exclusively online or through technology, or accompany face-to-face domestic and sexual violence. While there are many types of technology-facilitated violence, certain distinguishing features make it particularly damaging to the survivor:[54]

- **Accessibility:** abuse can be channelled through numerous readily available and affordable technologies.
- **Action-at-a-distance:** abuse can take place without physical contact, from anywhere, and enable perpetrators to convey a sense of omnipresence.
- **Automation:** abuse can require less time and effort.
- **Anonymity:** the perpetrator can remain unknown to their victim(s).
- **Propagation and perpetuity:** abusive content can multiply and exist for a long time, even indefinitely.

As technology evolves, so do the types of technology-facilitated violence. Currently, the most common types of technology-facilitated violence include:[55]

- **Cyber-harassment:** communicating with the victim against their will with the intent of causing harm. Within cyber-harassment fall:
  - **Trolling:** posting messages, images, videos, other online content, or creating online campaigns through hashtags to annoy a target or to incite violence against a person.[56]
  - **Gender trolling:** aggressive and coordinated attacks including gendered verbal abuse and intimidation, such as rape, death threats, and photos of homes and families, against women and 2SLGBTQIA+ people who speak against heteronormative patriarchal norms.[57]

An example of gender trolling is the experience of Anita Sarkeesian, a Canadian-American blogger, who criticized women's portrayal in video games and received sexist jokes, rape, death threats, and many pornographic drawings showing her being raped by video game characters. Her harassers also created a video game, Beat Up Anita Sarkeesian, which encouraged players to digitally cover a photo of Sarkeesian with blood by clicking the mouse.[58]

- **Swatting** (named after police SWAT teams)**:** calling 911 claiming the target is engaged in a dangerous activity (e.g., holding a hostage), to get dispatchers to send police to their location and intimidate them.[59] Swatting is particularly dangerous when used against racialized populations, especially Black Canadians and Indigenous Peoples, who are disproportionately affected by police brutality and more likely to suffer violence because of the call.
- **Zoombombing:** breaking into Zoom meetings, usually devoted to promoting the rights of equity-deserving populations and disrupting them by sharing sexually explicit and discriminatory messages and images. For example, in 2020, two prominent female journalists had to end their Zoom event focused on the challenges that female founders face in the

technology industry because a participant began broadcasting pornography.[60]

- **Cyber or online mobbing:** cyber-harassment perpetrated by a group of individuals using a variety of strategies.
  - ***Coordinated flagging campaigns*** involves driving content, individuals, or groups off the Internet by maliciously marking posted content as harmful and in need of removal.
  - ***Brigading*** involves manipulating algorithms to amplify harassment and boost harmful content. Examples include:
    - Using fake accounts to increase the popularity of a post ("sock puppetting");
    - Posting an excessive number of replies to a tweet to drown its retweets and likes and imply that the post has been poorly received ("rationing");
    - Disrupting online debates by repeatedly posting disingenuous questions ("sealioning");[61] or disrupting online campaigns by hijacking its hashtags and associating them with abusive material ("hashtag poisoning").[62] Online mobbing is usually used against activists and online communities of equity-deserving groups that promote human rights and social justice.
- **Online sexual harassment:** communication of sexual nature without consent. Examples include references to the targeted person's sexuality or sexual activity, sexualized insults, or shaming the person for their sexuality or sexual activity.[63]

An example of hashtag poisoning is the 2015 attempt to disrupt the #TakeBackTheTech and #ImagineAFeministInternet campaigns by the Internet Governance Forum through a coordinated flood of anti-feminist and misogynistic messages and memes.

- **Cyber-stalking and surveillance/tracking**: using both devices and platforms such as spyware or stalkerware, to monitor a victim's activities in real-time or historically. Even supposedly non-malicious apps, usually advertised for child or employee monitoring, are routinely repurposed into spyware and stalkerware to monitor private communications and online activities, text messages, phone calls, check browsing history, or track real-time location.[64] Many apps and devices are openly marketed to men who want to control their partners.[65] For example, in 2019, Highster Mobile, described their monitoring app as "the perfect tool to catch a cheating spouse."[66]
- **Online defamation:** spreading rumours online to discredit individuals or groups.
- **Doxing/doxxing**: releasing a victim's personal information online against their wishes, often used as an intimidation strategy against female activists to drive them off the Internet or against transgender users of dating sites to drive them off the platform.
- **Hacking/interception of private communication:** using technology to gain illegal or unauthorized access to systems or resources to acquire or modify personal information.[67]
- **Online hate speech:** statements or other content that convey misogynistic or harmful attitudes towards women, girls, and equity-deserving populations. On the Internet, there are entire online communities dedicated to misogynist speech. For example, the perpetrator of the 2018 Toronto

van attack spent time on Reddit incel subgroups and incel chat sites, sharing other members' frustration at not finding girlfriends, framed within the ideology of male entitlement.[68]

- **Image-based abuse** includes several types of technology facilitated violence:
  - **Non-consensual distribution of consensual images:** sharing photos accessed without the victim's consent. For example, 70,000 images of women were downloaded from the dating app Tinder and posted onto an online cyber-crime forum.[69]
  - **Non-consensual image creation:** obtaining illicit images, either through **voyeurism** (i.e., installing hidden cameras in public places or unlawfully accessing individuals' webcams or phone cameras without their consent or knowledge), or **upskirting** (i.e., placing phones or other image-capturing devices under women's skirts and taking images).
  - **Non-consensual image distribution:** livestreaming or sharing videos of sexual assaults, when either the perpetrator or the witnesses broadcast the abuse in real time or post-factum.
  - **Digitally altered non-consensual images:** creating **deepnudes** or images altered by photoshopping a victim's face onto a sexually explicit image.
  - **Digitally altered videos:** creating **shallow fakes** or **cheap fakes**, which tweak the existing material slightly (e.g., slowing the video to make the speaker look intoxicated), and **deepfakes**, which alter a video using sophisticated artificial intelligence (AI) and machine learning algorithms.

Approximately 96% of deepfakes represent pornographic videos with actresses' faces replaced with faces of ex-partners, other real women, or female celebrities.[70]

  - **Sextortion** or **sexual blackmail**: pressing a victim for sexually explicit photos or threatening to release sexually explicit photos, which may or may not exist, to the public. A notorious case of sextortion is cyber-harassment of Amanda Todd, whose accused cyberbully lured her to expose her breasts on a webcam and later demanded more explicit images under the threat of sharing the images he had with Amanda's family and friends.[71]

- **Impersonating:** using technology to assume a victim's identity to access private information, embarrass or shame the victim, or create fraudulent identity documents.
- **Luring and online exploitation:** communicating through technology to commit a sexual offence, for example, asking an individual to create or send naked or semi-naked sexual pictures or videos or exploiting an individual for sex work.[72] Online luring and exploitation drastically increased during the pandemic, where predators impersonate children or teenagers to exploit vulnerable individuals as children spend more time online. Often, predators use "attention bombing" (i.e., excessive communication and compliments) to gain their victims' trust before forcing them into risky behaviours.[73]
- **Non-consensual sexting:** sending sexually explicit images against the recipient's wishes. Sexting as a consensual activity involves sharing intimate images intentionally with partners or romantic interests and is equally common among women and men. However, women are more commonly

pressured or coerced into sending naked photos, while men are more likely to share women's images with others.[74]

- **Technology-facilitated coercive control**: use of social media and other digital platforms and communication technologies by intimate partners to intimidate, isolate, and control their partners or former partners, including by leveraging their own social networks to target the victim, while threatening, co-opting, and undermining the victim's own social networks.[75]

Because technological exclusion and technology-facilitated violence stem from the systems of oppression, i.e., the same roots as domestic and sexual violence, primary prevention must be comprehensive. It must include changing the **social norms and values** that normalize violence and inequity, present technology-facilitated violence as less harmful than face-to-face abuse, and place the responsibility for avoiding victimization onto girls, women, and equity-deserving groups rather than society, the information and communication technology sector, and the government. It must also ensure **equitable access to and participation in digital spaces and technology** for women and equity-deserving groups so that they engage in self-development and self-actualization. Finally, it must address the **specific features of technology and digital spaces** that increase the risk of technology-facilitated violence.

The next two sections provide recommendations for the Government of Alberta on legislation and policy reforms for technological and digital safety and inclusion while the third section outlines how Alberta's anti-violence sector, the IMPACT collective, can promote technological and digital safety and inclusion through its work. Government recommendations briefly touch on social norms and technological access reforms and focus on the technology-specific recommendations in more detail since this area is understudied.

For ease, we organize the recommendations under two domains: legislation and policy reforms. Legislation is an important component of prevention because it can serve as a deterrent for perpetrators. However, it is important to remember that many equity-deserving groups at risk of technology-facilitated violence cannot access legal remedies because of their costs, time, and survivors' unwillingness to deal with the criminal system due to the lack of trust and the threat of revictimization.[76] Therefore, policy reforms must emphasize the responsibility of all citizens, systems, and institutions, especially the ICT sector, to promote technological inclusion and prevent technology-facilitated violence.[77] Examples of how his can be accomplished include introducing mandatory digital literacy curricula in educational institutions; promoting a bystander approach in digital interactions in all organizations; ensuring data privacy for equity-deserving groups who rely on technology, such as seniors and people with disabilities; and ensuring the ICT sector eliminates harmful hardware and software that can be used for violence and introduces technological safeguards.[78]

4.0 Recommendations for promoting technological and digital inclusion and safety to prevent domestic and sexual violence

4.1 Rationale for legislation and policy reforms

Legislation reforms promoting technological inclusion and criminalizing new forms of technology-facilitated violence at the federal and provincial levels are essential. They signal that technological exclusion is a violation of human rights that increases social exclusion and opportunities to perpetrate violence. Additionally, they signal that technology-facilitated violence is not only an individual harm, but also a public wrong that violates victims' integrity, dignity, autonomy, and equality, and is worthy of public sanctions.[79] Legislation is also an important tool for showing commitment to promoting the empowerment of equity-deserving groups who are disproportionately affected by technology-facilitated violence.[80] Furthermore, legislation regulating online platforms and technological devices is crucial to ensure the ICT sector takes active preventative measures against violence and does its due diligence.

However, there are a number of challenges with regulating technology safety and inclusion through legal reforms. The most important concern about criminal law is its unintended impact. First, it may disproportionately affect equity-deserving populations, who are more likely to get reported, found guilty, and punished more severely compared to privileged groups.[81] Additionally, when criminal legislation is used against adolescents and youth, a conviction may derail their entire lives.[82] Therefore, legislation reforms must go hand-in-hand with capacity building for the criminal justice sector on cultural competency, anti-oppression, and working with equity-deserving groups, adolescents, and youth in empowering ways.

Another issue with legal regulation is that the Internet and technology evolve very quickly while introducing new laws that are evidence-based, evidence-informed, effective, just, and proportional requires time.[83] Therefore, working in partnership with technology makers and service providers is important to ensure their buy-in into a more equitable and safer technological and digital space by design.

Finally, legislating against technology-facilitated violence, specifically online hate speech and harassment, sometimes clashes with free speech provisions from the Canadian Charter of Rights and Freedoms. Legislation limiting harmful or abusive speech that does not qualify as hate incitement, or legislation defining technology-facilitated violence too broadly can be repealed as "excessive regulation." This was the case of Section 13 of the Human Rights Act against hate messages and the 2015 Nova Scotia Cyber-Safety Act.[84] Furthermore, increased controls imposed on websites and social platforms can be touted as government surveillance. Therefore, new legislation must be both carefully tailored and committed to protecting equity-deserving groups through measures informed by and respectful of equity-deserving groups' experiences, needs, and aspirations.

Policy reforms are essential as criminal sanctions and technology-regulating legislation are not enough for primary prevention of domestic and sexual violence. Broader socio-cultural, systemic, and institutional transformations are required.[85] Since the field of digital technology is relatively new and ever-evolving, research into the nature of technology-facilitated violence, its impacts, the most affected populations, emergent threats, and the most effective preventative measures is essential. Governments have a leading role to play in providing resources for the activities of various actors, such as academics, think tanks, and other organizations currently working on separate projects, and funding opportunities for knowledge dissemination. Governments should also coordinate partnerships and alliances within the industry. Furthermore, governments should work with educational institutions, workplaces, community groups, and organizations to ensure that best practices for technology-facilitated violence prevention are integrated within their spheres of activity through internal policies and procedures and professional capacity building. Finally, governments have the resources and responsibilities to facilitate social norms change by organizing large-scale public awareness campaigns against technological exclusion and technology-facilitated violence and in support of gender equality and social inclusion.

4.2 Legislation recommendations

4.2.1 Legislation recommendations to the Government of Canada

1. **Reinstate Section 13 of the Human Rights Act that stipulated a proactive human-rights based approach to identity-based online attacks**.[86]

Human rights remedies are essential for protecting targeted equity-deserving groups[87] and can serve as an important **mechanism for social norms change**, signalling a strong social opposition to online hate. In addition to facilitating norms change and **serving as a deterrent**, human rights remedies can increase the reporting of hateful speech because they do not require proof of blameworthy intent as criminal proceedings do, which often deters equity-deserving populations from reporting.[88] Additionally, they do not require any prior state authorization for filing a complaint, unlike Criminal Code provisions, which require the Attorney General's consent to initiate prosecution.[89] Furthermore, they can provide better protection for the rights of equity-deserving populations as the criminal legal system often prioritize values such as the freedom of expression, at the expense of equality concerns. Finally, human rights mechanisms can promote restorative remedies for complainants and education for perpetrators, unlike the criminal prosecutions focusing on punitive remedies.[90]

2. **Adapt the Criminal Code and other federal legislation to aid in preventing technology-facilitated violence and protecting vulnerable individuals.**[91]

It is essential to ensure that harmful and abusive uses of technology are criminally punishable to **serve as a deterrent** and that the legislation covers all possible uses of technology for domestic and sexual violence. To address this issue:

- In criminal laws, use **adequate thresholds of culpability**,[92] (e.g., do not use the intent to distress as a requirement for an act to be declared criminal), and **address the rights of equity-deserving groups** (e.g., focus on adolescents and youth, not only on prepubescent children) when planning the prevention of online sexual exploitation.[93]
- **Lower the threshold of sensitivity** in defining image-based abuse so that images that do not currently meet criminal law definitions, but are part of the continuum of abuse, are banned, blocked, and removed. For example, criminalize all images associated with an abusive incident, including images that are not abusing but were taken immediately prior to abuse, and nude or partially nude images of children that were created and shared legally, e.g., by children's parents on social media, but are used in a sexualized context or connected to sexual commentary, e.g., on child abuse sites.[94]
- **Criminalize non-consensual deepnudes and sexual deepfakes.**[95] For now, legal responses include defamation, appropriation of personality, and Canadian Elections Act laws, depending on the context. Criminalization of non-consensual deepnudes and sexual deepfakes will serve as a stronger deterrent and better enable the attribution of liability since law enforcement agencies have greater investigative capacities than private individuals or lawyers.
- Ensure that **child pornography laws do not apply to youth** who create a nude or sexually explicit image of *themselves* and share it with someone of their choosing.[96] Youth who distribute intimate images of *other* youth without consent should be charged under the offence of non-consensual distribution of intimate images, but not under the Criminal Code's child pornography provisions, except in extreme circumstances, for example, where image production involves sexual exploitation or distribution is done for profit.

3. **Close all legal loopholes that have enabled companies to evade liability for the technological exclusion and technology-facilitated violence they facilitate on their platforms or through their apps, software, or devices.**[97]

It is important to hold technology producers and service providers accountable for allowing their products and services to be misused for exclusion and violence. Presently, a platform cannot be held liable for technology-facilitated violence committed by users and has no legal obligation to act unless (1) the user's post meets the legal definition of defamation or copyright infringement; (2) the platform can be sued under a general application law; or (3) the platform's involvement meets the bar either for "enabling" copyright violations or for direct liability due to being party to a criminal case of technology-facilitated violence.[98] To address this issue:

- Update the Federal Privacy Commissioner's purview[99] to **compel technology producers and service providers to modify their policies and practices** instead of only recommending voluntary changes, including by issuing Administrative Monetary Penalties[100] and offering incentives.
- Introduce statutory **Duty to Act Responsibly** imposing an affirmative requirement on platforms, including social media companies, large messaging groups, search engines, and other Internet operators involved in the dissemination of user-generated and third-party

content[101] to review their products and implement proactive modifications for preventing technological exclusion and technology-facilitated violence.

- Enact one or more versions of the current **"enabler" provisions in subsections 27(2.3) and 27(2.4) of the Copyright Act**, adapted specifically to address different forms of technology-facilitated violence,[102] including "purpose-built"[††] platforms that exist predominantly to host, solicit, generate, and/or facilitate technology-facilitated violence by users.
- Establish the **legality of covert spyware and stalkerware apps,**[103] even those marketed for children monitoring, on a case-by-case basis, to ban the apps predominantly used for technology-facilitated violence.
- Reinforce legislation to ensure that legal stalkerware companies operating in Canada fall under privacy legislation, PIPEDA,[‡‡] and that they **amend their collection, use, or disclosure of personal information in line with PIPEDA** to ensure user privacy.[104]
- Introduce legislation to **limit the amount of personal data available to website and social media owners, and technology and service providers** to ensure that users, especially from equity-deserving groups, are not driven off the Internet and prevented from seeking vital information that can protect them from violence because they are threatened by their data being collected, used, and exposed.[105] The current-data-for-services model of the Internet not only endangers people's privacy but also potentially increases social divisions when data is mined for political advertising and public opinion manipulation, which often threatens the safety of equity-deserving populations.[106] Special attention should be paid to ensure **children's data protection.** Create no-go zones prohibiting profiling children for marketing purposes and other invasive practices. Corporations must only collect and use data for service provision and delete all data after proving the service. [107]
- In line with the Privacy Commissioner of Canada's Draft Position on Online Reputation (2018), pass legislation to **provide children with a right to be forgotten.** (i.e., online information or content posted by their parents or guardians can be deindexed from search engines and/or taken down upon children's request when they reach the age of majority).[108]

[††] "Purpose-built" means designed to meet specific business requirements due to specific individual and/or mobile application requirements. They are not over-built for the sake of trends. See Howland, S. (2012). *Purpose-built vs built for a purpose: What's the difference*. https://www.fieldtechnologiesonline.com/doc/purpose-built-vs-built-for-a-purpose-0001

[‡‡] Office of the Privacy Commissioner of Canada. (n.d.). *Personal information protection and electronic documents act (PIPEDA)*. https://www.priv.gc.ca/en/privacy-topics/privacy-laws-in-canada/the-personal-information-protection-and-electronic-documents-act-pipeda/

4.2.2 Legislation Recommendations to the Government of Alberta

1. **Introduce specific legislation on technology-facilitated violence where Alberta has authority.**[109]

While such legislation would facilitate reporting and responding to technology-facilitated violence, it would also contribute to primary prevention by: 1) signalling the government's commitment to technological inclusion and eradication of technology-facilitated violence; and 2) deterring perpetrators. To address this issue:

- Create a **new civil wrong of technology-facilitated harassment**[110] that would stand for intentional infliction of emotional distress by means of technology and cover: (1) outrageous technology facilitated conduct; (2) intention of causing emotional distress or reckless disregard of causing emotional distress by means of technology; (3) suffering of severe or extreme emotional distress; and (4) the actual and proximate causation of the emotional distress by the perpetrator's outrageous conduct.
- Create a **targeted cyberbullying tort**[111] that would define it as a crime to deter perpetrators and allow victims to sue if they suffer repeated communication through technology that is intended or can be reasonably expected to cause fear, intimidation, humiliation, extreme distress, other damage, or harm to their physical or psychological health. The new law must include a power for judges to make prevention and victim compensation orders.
- Broaden the **tort of the Privacy Act** to include the unauthorized use of someone's name or image for the purpose of harassing, humiliating, distressing, or exposing them to ridicule or contempt online or through technology.[112]
- Broaden the definition of **illegal content** to include that which may not be criminal in itself but that remains severely harmful or abusive (e.g., images of children in bathing suits or distributed on forums dedicated to sexualizing children; sexual commentary related to an image, video, or description of a child; or releasing a child's personal information).[113] Ensure that prevention of harmful and abusive content includes speech-based violence,[114] since in many cases it requires a higher burden of proof to be classified as violence and its perpetration is treated more leniently.
- Implement robust legislation to regulate technology developers, producers, and sellers, as well as electronic, technological, and communication service providers operating at the provincial level to ensure their **ethical conduct and the integration of preventative measures** to reduce the risks of their products and services being from used for technology-facilitated violence.[115] Legally mandate greater transparency and accountability and increase developers', producers', and sellers' responsibility to uphold citizens' rights to privacy, safety, respect, dignity, and autonomy.[116] Since current voluntary mechanisms lead to under-enforcement,[117] duty of care, or at least some crucial mechanisms, must be made compulsory,[118] along with financial penalties for non-compliance and incentives for fulfilling duty of care properly.
- Ban the creation, marketing, sale, purchase, and use of unwarranted monitoring devices, keyloggers,[119] illicit GPS and IP trackers, "stalking" apps,[120] software, and other forms of **technology that can be used to invade the privacy of computers, phones, and other**

technology to monitor people's online and offline activities, communications, and geographic location. Legally compel app stores and online intermediaries to proactively enforce their policies and developer agreements against stalkerware,[121] including by regularly conducting a full app store sweep and issuing public recalls (e.g., through push notifications to mobile devices that have banned apps installed). Additionally, fund research by academics and non-profit organizations to identify such technology and organize public awareness-raising campaigns about them.[122]

- **Legislate an Opt-In model** based on the highest level of content safety for all websites and apps with adult or sensitive content, which would require information and communication technology service providers to block access to pornography websites and websites and apps with sexually explicit, violent, and extreme harmful and abusive content by default; require multi-stage registration procedures for accessing them; and implement strict guidelines and enforcement of terms of use.[123]

4.3 Policy recommendations

4.3.1 Policy recommendations to the Government of Canada

1. Establish a **national expert regulator on technology-facilitated violence with a dual mandate**[124] to lead **research and education** on technology-facilitated violence and to **promote legal and policy remedies** for prevention and response to it.

2. Establish a new **office for protecting and promoting the rights of girls, women, and equity-deserving groups online and on technological devices.**[125] The office must be independent of government but housed within the federal Ministry for Women and Gender Equality, and must conduct research, facilitate dialogue, and make recommendations to government about appropriate legal and policy reforms for promoting technological inclusion and preventing technology-facilitated violence against populations at risk. Women and equity-deserving groups must act as fully resourced, respected participants in the research and policy-making processes.

3. **Establish a new regulatory body to address medium-term and long-term policy issues related to online platforms**[126] **(**e.g., platform governance and content moderation). The regulatory body must work with social media platforms, selecting case-based strategies for implementing a code of conduct to prevent technology facilitated violence, and integrating the recommendations made by researchers, civil society, and other interested parties.

4.3.2 Policy recommendations to the Government of Alberta

1. **Increase the technological inclusion of women and equity-deserving groups, addressing their unique needs and vulnerabilities, such as risk factors for domestic and sexual violence.**

    - Develop and implement a **digital and technological access strategy** for women and equity-

deserving group [127] and a comprehensive **digital strategy for rural and remote communities.**[128, 129]

- Fund **digital infrastructure** [130] and better **access to high-speed networks** in rural and remote areas,[131] addressing the **overreliance on satellite connectivity** that may create vulnerabilities in northern Alberta.[132]
- Establish **pricing benchmarks** for broadband services[133] and cover the cost of **Internet connection,**[134] **technology,**[135] and **cell phone data plans**[136] for low-income women and equity-deserving populations[137] to participate in education, the workforce, and the socio-cultural life of their communities.[138]
- Establish **scholarships, paid internships, fellowships, professional networking, and mentorship opportunities** and incentives for the ICT sector to increase the number of girls, women, and equity-deserving populations in the sector and improve its culture.[139]
- Invest in **age-friendly and accessible digital innovation and technology development** for health, social care, education, and employment. For example, provide funding and grants for Alberta start-ups, incubators, and researchers working on technological and digital products and services that can benefit equity-deserving groups.[140]
- Require local manufacturers to use universal design principles for **digital and technological accessibility,**[141] digital services providers and technology developers to implement **age-friendliness and accessibility standards,** [142] and vendors to demonstrate that their **technological and digital products are accessible** to users with disabilities.[143]
- Mandate all **essential public websites to provide accessible information** for people with disabilities.[144]
- Cover the costs of **assistive technology** required in school or at work,[145] **home security devices,**[146] and **assistive technologies** that facilitate ageing in place and independent living for seniors and people with disabilities.[147]
- Invest in developing **telemedicine and tele-home care programs** that allow healthcare providers to diagnose, treat, and monitor patients virtually.[148] Fund initiatives that use technology and digital spaces to offer **social services** to rural women and equity-deserving populations[149] and to increase people's **civic participation** and **social activities** that counter isolation.[150, 151]
- Establish stable long-term funding for organizations promoting **technological inclusion of equity-deserving groups**, their rights online, [152] as well as digital literacy, critical media skills, and technology-facilitated violence prevention.[153]
- Fund **innovative and creative online resources, apps, and technological devices**[154] for youth and adults to develop online safety and initiatives that leverage technology to enhance girls', women, and equity-deserving groups' safety.

2. **Establish and provide long-term stable funding to an Alberta-based research consortium on technological inclusion and technology-facilitated violence.**

   A collective of academics, legal scholars and professionals, technology and security specialists, the ICT sector, violence prevention organizations, survivors, and activists must carry out

research and knowledge dissemination. Topics to focus on are: provincial technology-facilitated violence trends,[155] emergent threats to technological inclusion and safety, best technological prevention strategies,[156] and best legal and political prevention strategies.[157]

3. **Establish and provide long-term, stable funding to a legislation and policy review committee on technological inclusion and safety.**[158]

   The committee must regularly review all the provincial legislation and policy on technological inclusion and technology-facilitated violence to identify gaps, propose solutions, and consult the government on their implementation.[159]

4. **Establish a provincial expert regulator on technological inclusion and technology-facilitated violence with regulatory and enforcement powers.** [160]

   The regulator must implement the recommendations by the research consortium and the legislation and policy review committee on technological inclusion and technology-facilitated violence.

5. **In collaboration with equity-deserving groups, develop binding policies for the ICT sector**.

   - Cooperate with and fund the ICT sector to develop and implement **AI to increase technological inclusion and safety**.[161]
   - Require the ICT sector to **seek feedback from girls, women, and equity-deserving populations**[162] at the design and testing stages of their products, and to make necessary modifications to mitigate potential risks.
   - Require ICT service providers to **use encryption** to protect users' information and generated content,[163] especially equity-deserving groups or those at risk of violence,[164] including journalists, researchers, lawyers, and civil society activists.[165]
   - Require the ICT sector to **limit their collection and sharing of users' data and location**. This is accomplished by turning off location services and photo location by default, removing GPS and EXIF from uploaded photos by default,[166] and **refraining from sharing users' information with third-party platforms** by controlling outside access to the application programming interface to prevent malicious code or third-party apps from compromising their privacy system.[167]
   - Require the ICT sector to create **non-negotiable minimum base standards for harmful content** and how to report their violation,[168] ensuring that these standards do not negatively impact equity-deserving groups. For example, reporting mechanisms must ensure that they cannot be used as a tool of oppression against 2SLGBTQIA+ individuals, who are often flagged, reported, and banned from social media due to homophobia, biphobia, and transphobia rather than due to violating social media rules.
   - Require the ICT sector to establish better regulations for **platforms accepting user-generated content,** especially containing sex and nudity. For example, require proof of

subject's age, participant's consent for both recording and distribution of the uploaded content, and uploader verification.[169]

- Require the ICT sector to **segregate children and adults in the digital and technological space by design** or, when impossible, to implement additional measures to prevent children from accessing adult or mature content.[170]
- Require the ICT sector to establish clear standards for a minimum **effective automated detection strategy** and to implement automated proactive content detection and blocking for platforms and apps with user-generated content.[171] Incentivize large ICT service providers to help small service providers implement the same proactive automated content detection measures, especially for image and file hosting services.[172]
- Require the ICT sector to outline **minimum base standards for user-reporting mechanisms** to flag and report harmful-abusive content, contact content administrators, and lodge complaints,[173] as well as **minimum base standards for quick responses** to complaints.[174] Service providers must regularly update reporting mechanisms and ensure that harmful content be automatically removed from the platform's parent, subsidiary, or sibling platform companies where the same content also appears.[175]
- Require that companies providing dual-use products or services[176] (i.e., used both for legitimate purposes and for technology-facilitated violence), implement **binding protocols for duty of care** by proactively implementing effective measures to mitigate the risks of product and service misuse.[177]
- Require dating app developers to **fight sexism, racism, colonialism, and other types of discrimination actively** on their apps. For example, eliminate bias from algorithms to expose users to matches from all backgrounds rather than only their own backgrounds.[178]
- Limit the amount of personal data available to investigators working on technology-facilitated violence to prevent them from exploiting it for personal use, as some investigators leverage state surveillance tools to stalk former partners or to engage in other forms of professional misconduct, a practice known within the intelligence community as **LOVEINT.**[179]
- Require the ICT sector to **undergo independent audits**[180] **on technological inclusion and safety**, to make amendments, and publish comprehensive annual transparency reports.
- Require the ICT sector to submit regular **public risk assessment reports** (e.g., on algorithm safety), automated and manual content moderation techniques, and **incident reports**,[181] including when requested by the media, researchers, and policy communities.[182]

6. **In cooperation with equity-deserving groups, develop binding policies for educational institutions, workplaces, community organizations, religious organizations, human service providers, etc., on ensuring technological inclusion and safety.**[183]

   Require all institutions and organizations to adapt, implement, monitor, and evaluate evidence-based and evidence-informed policies and procedures for technological inclusion and safety that would encourage positive digital spaces; promote good digital citizenship; outline the allowed uses of information and communication technology; establish monitoring

and evaluation plans; and specify measures against inappropriate or violent online or technology-facilitated behaviour.[184]

7. **Require all early childhood development institutions, schools, colleges, universities, and extracurricular activity organizations to implement high-quality age- and activity-appropriate curricula on children's rights and digital and critical media literacy,[185] including pornography literacy.[186]**

   Curricula must help children and youth see themselves as rights bearers and empower them to exercise their rights, including the right to privacy, access to information, freedom from discrimination, and participation in decision-making in matters affecting them.

8. **Change social norms and perceptions of group norms by creating a sustainable network of government agencies, private sector organizations, community organizations, human service providers, and other organizations serving girls, women, and equity-deserving populations to develop and implement innovative social norms initiatives on technological inclusion and safety.[187]**

   - Organize **educational campaigns** on technological exclusion and technology-facilitated violence as grave social problems, indicating the government and other stakeholders take these issues seriously.[188] Raise awareness that technology-facilitated violence is a form of violence,[189] equally dangerous, socially costly,[190] and harmful[191] as other forms of violence, and a human rights violation that can be legally punishable,[192] focusing on the types of technology-facilitated violence currently perceived as more acceptable. Additionally, raise awareness that viewing, redistributing, or otherwise engaging with harmful and abusive speech and non-consensually shared images means participating in abuse.[193]
   - Promote **positive digital citizenship, positive peer pressure** and an **engaged bystander approach** to technological inclusion and safety[194] by empowering individuals and groups to promote positive norms of empathy and respect in technology-facilitated interactions.[195] This includes challenging aggression and violence, misogyny, and other forms of oppression[196] and the practices that are not illegal but still harmful and abusive.[197] Invite celebrities, influencers, politicians, and other actors to serve as role models of healthy online and technology-facilitated interactions and ethical digital citizenship.[198]
   - Fund initiatives that promote the **rights of girls, women, and equity-deserving populations to participate and self-express online and through technology**,[199] including in traditionally white, heterosexual, masculine spaces, such as online gaming communities or chatrooms.[200] Raise awareness about girls', women's, and diverse populations' challenges in online and technology-facilitated interactions[201] and the societal costs of their retreat from digital spaces, such as the reduced quality of civil society, politics, journalism, and culture.[202] Challenge the discourses that put the responsibility for technological inclusion and safety on girls, women, and equity-deserving populations rather than society as a whole.[203]

- Fund initiatives that **promote positive masculinity in online and technology-facilitated interactions and spaces,**[204] challenging online and technology-facilitated rape culture myths and toxic masculinity expressions.[205] Address the manosphere[206] by challenging views in a non-confrontational manner and engaging male champions of change, celebrities, influencers, and former members of the manosphere to encourage critical examination and to change viewpoints. Offer initiatives and spaces that allow boys and men to increase their self-esteem in positive ways, develop a sense of belonging to healthy and respectful communities, address their concerns and meet their needs, and foster empathy towards others.[207]

9. **Support institutional change by building the capacity of professionals working with women, equity-deserving groups, and the ICT sector.**

- Mandate capacity building for decision-makers, policy makers, and criminal justice professionals to change social norms around technology-facilitated violence from being a minor violation to one that is more significant[208] and improve their legal literacy on technological and digital safety legislation as well as their digital literacy.[209]
- Fund capacity building for educators, psychologists, social workers, human resources in educational institutions and workplaces, and other professionals working with girls, women, and equity-deserving populations to recognize technological exclusion and technology-facilitated violence as grave problems and to promote positive digital citizenship and positive peer pressure in online and technology-facilitated interactions through their professional practice.[210]
- Develop trainings and resources for mass media to apply best practices when reporting on technology-facilitated violence[211] and to use such reports for changing social norms around it.
- Mandate capacity building for the provincial ICT sector to ensure it recognizes technological exclusion and technology-facilitated violence as grave problems and addresses the risks through its work.

It is essential to add that, since technological and digital safety is an emergent area, there are still significant gaps in individual knowledge, skills, and abilities related to technology-facilitated violence. Therefore, in addition to systemic, institutional, and social norms change, the government and other stakeholders must also invest in increasing people's understanding of technological exclusion and technology-facilitated violence and improving individual capacity to prevent and address them.

4.3.3 Policy recommendations for the IMPACT collective

While the government must play the leading role in many reforms for technological inclusion and safety, the IMPACT collective members can contribute to the effort by:

- **Building the capacity of the anti-violence sector** in digital literacy and legislation related to promoting technological inclusion and safety.[212]

- Implementing **organizational policies and procedures for technological inclusion and safety**.[213]
- Increasing the **accessibility of their online and technology-assisted services** for women and equity-deserving groups, for example, by providing accessible information for people with disabilities on their websites[214] and offering services online and via technology.[215]
- Collecting data from technology-facilitated violence survivors who use their services and sharing it with the government and the ICT sector to **inform legislation and policy reforms**.
- Implementing **research and knowledge dissemination** on technology-facilitated violence among service users[216] and contributing expertise to provincial legislation and policy reviews on technological inclusion and technology-facilitated violence.[217]
- Organizing **educational campaigns** on technological exclusion and technology-facilitated violence as grave social problems and promoting positive norms.[218]
- Integrating curricula on children's rights and digital and critical media literacy,[219] including pornography literacy,[220] into programs for children and youth.
- Implementing initiatives that promote the **rights of girls, women, and equity-deserving populations** to technological inclusion and safety,[221] and promoting **positive masculinity in online and technology-facilitated interactions and spaces.**[222]
- **Advocating for legislation and policy reforms** from the government and the ICT sector.

5.0 Conclusion

Technological exclusion must be recognized as an important contributing factor to domestic and sexual violence. Furthermore, technology-facilitated domestic and sexual violence must be prioritized in primary prevention efforts as one of the most quickly growing types of victimization. It is important to address how the systems of oppression lead to technological exclusion, e.g., through advertisement-driven digital spaces, and how the drivers of violence shape technological and digital spaces, e.g., through social norms that downplay the risks and harms of technology and expect women and equity-deserving groups to ensure their own safety online. All action for technological safety and inclusion must be cross-jurisdictional, multi-sectoral, and comprehensive, encompassing legislative changes, policy reforms, active collaboration with the information and communication sector, awareness raising and public education, capacity building, and community mobilization for safe and inclusive technology and digital spaces. Because technological exclusion and technology-facilitated violence are particularly pervasive and vicious against women and equity-deserving groups, their safety, wellbeing, and empowerment must be centred in all primary prevention efforts.

References

[1] Flood, M [@MichaelGLFlood]. (2020, December 14). *So if we want to make…[Tweet]. Twitter. https://twitter.com/MichaelGLFlood/status/1338668780650557443*
[2] Lee, L., Wells, L., & Litviniuc, A. (2023). *Guiding the design of the Alberta primary prevention framework: A synthesis of shift's research to date from summer 2020-spring 2022.* Calgary, AB: The University of Calgary, Shift: The Project to End Domestic Violence.
[3]Lawson, T., and Garrod, J. (2001). *Dictionary of sociology*. London; Chicago: Fitzroy Dearborn.
[4] Lawson, T., and Garrod, J. (2001). *Dictionary of sociology*. London; Chicago: Fitzroy Dearborn.
[5] Newkirk, V. R. (October 6, 2017). *The Language of white supremacy*. The Atlantic. https://www.theatlantic.com/politics/archive/2017/10/the-language-of-white-supremacy/542148/
[6] Scott, J. (2014). *A dictionary of sociology.* Oxford: Oxford University Press; Fourth edition.
[7] Lohr, S. (2022). *Economists pin more blame on tech for rising inequality*. The New York Times. https://www.nytimes.com/2022/01/11/technology/income-inequality-technology.html
[8] Lowrey, A. (2021, April). *Low-skill workers aren't a problem to be fixed. The Atlantic.* https://www.theatlantic.com/ideas/archive/2021/04/theres-no-such-thing-as-a-low-skill-worker/618674/
[9] Kaukinen, C. E., & Powers, R. A. (2015). The role of economic factors on women's risk for intimate partner violence. *Violence Against Women*, *21*(2), 229–248. https://doi.org/10.1177/1077801214564686
[10] Ragnedda, M., Ruiu, M. L., & Addeo, F. (2022). The self-reinforcing effect of digital and social exclusion: The inequality loop. *Telematics and Informatics*, *72*, 101852–. https://doi.org/10.1016/j.tele.2022.101852
[11] Rubinstein, C. (2022). *Does Innovation Engender Equality? Gender Inequality In Tech, Apparently, Is Still A Thing. Forbes. https://www.forbes.com/sites/carrierubinstein/2022/03/29/does-innovation-engender-equality-gender-inequality-in-tech-apparently-is-still-a-thing/?sh=42eef1652d03*
[12] Kapin, A. (2020). *Sexual harassment in Silicon Valley: Still rampant as ever*. https://www.forbes.com/sites/allysonkapin/2020/09/15/sexual-harassment-in-silicon-valley-still-rampant-as-ever/?sh=5de93d3d2cc4
[13] Mikkelson, S. (2021). *Gender Bias in Data and Tech.* Engineering for Change. *https://www.engineeringforchange.org/news/gender-bias-data-tech/*
[14] Aiston, J. (2021). *What is the manosphere and why is it a concern?* https://www.internetmatters.org/hub/news-blogs/what-is-the-manosphere-and-why-is-it-a-concern/
[15] Trudell, A.L. & Whitmore, E. (2020). *Pandemic meets Pandemic: Understanding the Impacts of COVID-19 on Gender-Based Violence Services and Survivors in Canada.* Ottawa & London, ON: Ending Violence Association of Canada & Anova.
[16] Lorenz, T. (2020). *'Zoombombing': When Video Conferences Go Wrong.* New York Times. https://www.nytimes.com/2020/03/20/style/zoombombing-zoom-trolling.html
[17] Patel, U., & Roesch, R. (2022). The prevalence of technology-facilitated sexual violence: A meta-analysis and systematic review. *Trauma, Violence, and Abuse, 23*(2), 428-443. https://doi.org/10.1177/1524838020958057
[18] Stevenson, M. (2019). *Technologically-facilitated violence against women and girls: The Canadian compromise.* International Human Rights Internship Program Working Paper Series, Vol. 7, No. 1. https://www.mcgill.ca/humanrights/files/humanrights/ihri_v7_2019_stevenson.pdf.9_stevenson.pdf
[19] The Liberal Party of Canada. (n.d.). *Protecting Canadians from online harms.* https://liberal.ca/our-platform/protecting-canadians-from-online-harms/
[20] Bilodeau, H., Kehler, A., & Minnema, N. (2021). *Internet use and COVID-19: How the Pandemic increased the amount of time Canadians spend online.* Statistics Canada. https://www150.statcan.gc.ca/n1/pub/45-28-0001/2021001/article/00027-eng.htm
[21] Trudell, A.L. & Whitmore, E. (2020). Pandemic meets pandemic: *Understanding the impacts of COVID-19 on gender-based violence services and survivors in Canada.* Ottawa & London, ON: Ending Violence Association of Canada & Anova.
[22] Statistics Canada. (2021). *After five years of increases, police-reported crime in Canada was down in 2020, but incidents of hate crime increased sharply.* The Daily. *https://www150.statcan.gc.ca/n1/daily-quotidien/210727/dq210727a-eng.htm*

[23] Statistics Canada. (2021). *After five years of increases, police-reported crime in Canada was down in 2020, but incidents of hate crime increased sharply.* The Daily. *https://www150.statcan.gc.ca/n1/daily-quotidien/210727/dq210727a-eng.htm*
[24] Khoo, C. (2021). *Deplatforming misogyny: Report on platform liability for technology-facilitated gender-based violence.* Women's Legal Education and Action Fund. https://www.leaf.ca/wp-content/uploads/2021/04/Full-Report-Deplatforming-Misogyny.pdf
[25] Horwitz, J. (2020). The Facebook files: A wall street journal investigation. *The Wall Street Journal.* https://www.wsj.com/articles/the-facebook-files-11631713039
[26]Canadian Women's Foundation. (2018). *Digital diversity: Together we can improve tech for everyone*. https://canadianwomen.org/blog/digital-diversity-together-we-can-improve-tech-for-everyone/
[27] Khoo, C. (2021). *Deplatforming misogyny: Report on platform liability for technology-facilitated gender-based violence.* Women's Legal Education and Action Fund. https://www.leaf.ca/wp-content/uploads/2021/04/Full-Report-Deplatforming-Misogyny.pdf
[28] Gender and the Economy. (2018). Nowhere to hide: The impact of technology facilitated violence, abuse, and harassment: https://www.gendereconomy.org/nowhere-to-hide-the-impact-of-technology-facilitated-violence-abuse-and-harassment/
[29] Biros-Bolton, N. (2021). *Tech-facilitated violence*. Women's Legal Education and Action Fund (LEAF). https://www.leaf.ca/publication/tech-facilitated-violence/
[30] Canadian Women's Foundation. (2019). *Online hate and cyberviolence.* https://canadianwomen.org/the-facts/online-hate-and-cyberviolence/
[31] Gecco, L. (2021). *Canadian 'incel' killer found guilty of murder over Toronto van attack.* The Guardian. https://www.theguardian.com/world/2021/mar/03/toronto-van-attack-guilty-murder
[32] Gladu, M. (2017). Taking action to end violence against young women and girls in Canada: Report of the standing committee on the status of women. https://www.ourcommons.ca/Content/Committee/421/FEWO/Reports/RP8823562/feworp07/feworp07-e.pdf
[33] Bailey, J. & Mathen, C. (2019). Technology-facilitated violence against women & girls: Assessing the Canadian criminal law response. *Canadian Bar Review, 97(3),* 564. https://cbr.cba.org/index.php/cbr/article/view/4562/4468
[34] Bailey, J., Steeves, V. & Dunn, S. (2017). Submission to the special rapporteur on violence against women, Re: Regulating online violence and harassment against women, Submission to the United Nations Special Rapporteur on Violence Against Women. http://www.equalityproject.ca/wp-content/uploads/2017/12/Bailey-Steeves-Dunn-Submission-27-Sep-2017.pdf
[35] Dunn, S. (2020). Technology-facilitated gender-based violence: An overview. Supporting a Safer Internet Paper No. 1, Centre for International Governance Innovation. https://www.cigionline.org/static/documents/documents/SaferInternet_Paper%20no%201_0.pdf
[36] Deibert, R. J. (2017). *Submission of the citizen lab (Munk school of global affairs, university of Toronto) to the United Nations special rapporteur on violence against women, its causes and consequences, Ms. Dubravka Šimonović*. https://citizenlab.ca/wp-content/uploads/2017/11/Final-UNSRVAG-CitizenLab.pdf
[37] Biros-Bolton, N. (2021). *Tech-facilitated violence.* Women's Legal Education and Action Fund (LEAF). https://www.leaf.ca/publication/tech-facilitated-violence/
[38] Gender and the Economy. (2018). *Nowhere to hide: The impact of technology facilitated violence, abuse, and harassment.* https://www.gendereconomy.org/nowhere-to-hide-the-impact-of-technology-facilitated-violence-abuse-and-harassment/
[39] Bailey, J. & Mathen, C. (2019). Technology-facilitated violence against women & girls: Assessing the Canadian criminal law response. *Canadian Bar Review, 97(3),* 564. https://cbr.cba.org/index.php/cbr/article/view/4562/4468
[40] Biros-Bolton, N. (2021). *Tech-facilitated violence.* Women's Legal Education and Action Fund (LEAF). https://www.leaf.ca/publication/tech-facilitated-violence/.
[41] Biros-Bolton, N. (2021). *Tech-facilitated violence.* Women's Legal Education and Action Fund (LEAF). https://www.leaf.ca/publication/tech-facilitated-violence/.
[42] Canadian Radio-television and Telecommunications Commission. (2022). *Broadband Fund: Closing the digital divide in Canada.* https://crtc.gc.ca/eng/internet/internet.htm
[43] Technology Helps. (2021). *What is technology poverty?* https://technologyhelps.org/resources/what-is-technology-poverty/

[44] Technology Helps. (2021). *What is technology poverty?* https://technologyhelps.org/resources/what-is-technology-poverty/.
[45] Weeden, S. A. & Wayne, K. (2021). The digital divide has become a chasm: Here's how we bridge the gap. Centre for International Governance Innovation. https://www.cigionline.org/articles/the-digital-divide-has-become-a-chasm-heres-how-we-bridge-the-gap/
[46] Ahmed, N.& Harper-Merrett, T. (2021). The 'digital divide' is about equity, not infrastructure. https://policyresponse.ca/the-digital-divide-is-about-equity-not-infrastructure/
[47] Lortie. J., Morgan, C. S., & Bouthillier, S. (2021). A Province cannot compel internet service providers to block access to websites: Online communications fall under exclusive federal jurisdiction. https://www.mccarthy.ca/en/insights/blogs/consumer-markets-perspectives/province-cannot-compel-internet-service-providers-block-access-websites-online-communications-fall-under-exclusive-federal-jurisdiction
[48] Khoo, C. (2021). *Deplatforming misogyny: Report on platform liability for technology-facilitated gender-based violence.* Women's Legal Education and Action Fund. https://www.leaf.ca/wp-content/uploads/2021/04/Full-Report-Deplatforming-Misogyny.pdf
[49] Lalonde, D. (2021). Policy options on non-consensual deepnudes and sexual deepfakes. *Learning Network Brief 39.* London, Ontario: Learning Network, Centre for Research & Education on Violence Against Women & Children. https://www.vawlearningnetwork.ca/our-work/briefs/briefpdfs/Learning-Network-Brief-39.pdf
[50] Story, D. (2022). *The ethics of deepfake pornography.* Public Ethics. https://www.publicethics.org/post/the-ethics-of-deepfake-pornography
[51] Bailey, J. & Mathen, C. (2019). Technology-facilitated violence against women & girls: Assessing the Canadian criminal law response. *Canadian Bar Review, 97(3)*, 564. https://cbr.cba.org/index.php/cbr/article/view/4562/4468
[52] Public Safety Canada. (2021). *Child sexual exploitation on the internet*. https://www.publicsafety.gc.ca/cnt/cntrng-crm/chld-sxl-xplttn-ntrnt/index-en.aspx
[53] Canadian Women's Foundation. (2019). Online Hate and Cyberviolence. https://canadianwomen.org/the-facts/online-hate-and-cyberviolence/
[54] Lalonde, D. (2021). Policy options on non-consensual deepnudes and sexual deepfakes. *Learning Network Brief 39*. London, Ontario: Learning Network, Centre for Research & Education on Violence Against Women & Children. https://www.vawlearningnetwork.ca/our-work/briefs/briefpdfs/Learning-Network-Brief-39.pdf
[55] Khoo, C. (2021). *Deplatforming misogyny: Report on platform liability for technology-facilitated gender-based violence.* Women's Legal Education and Action Fund. https://www.leaf.ca/wp-content/uploads/2021/04/Full-Report-Deplatforming-Misogyny.pdf
[56] Khoo, C. (2021). *Deplatforming misogyny: Report on platform liability for technology-facilitated gender-based violence.* Women's Legal Education and Action Fund. https://www.leaf.ca/wp-content/uploads/2021/04/Full-Report-Deplatforming-Misogyny.pdf
[57] Biros-Bolton, N. (2021). *Tech-facilitated violence*. Women's Legal Education and Action Fund (LEAF). https://www.leaf.ca/publication/tech-facilitated-violence/
[58] Reporters without Borders. (2018). *Women's rights: Forbidden subject*. https://rsf.org/sites/default/files/womens_rights-forbidden_subject.pdf
[59] Khoo, C. (2021). *Deplatforming misogyny: report on platform liability for technology-facilitated gender-based violence.* Women's Legal Education and Action Fund. https://www.leaf.ca/wp-content/uploads/2021/04/Full-Report-Deplatforming-Misogyny.pdf
[60] Lorenz, T. (2020). *'Zoombombing': When video conferences go wrong.* The New York Times. https://www.nytimes.com/2020/03/20/style/zoombombing-zoom-trolling.html
[61] Andrews, P. (2021). *Social media futures: What is brigading?* Tony Blair Institute for Global Change. https://institute.global/policy/social-media-futures-what-brigading
[62] Pen America. (2021). *Online harassment field manual*. https://onlineharassmentfieldmanual.pen.org/defining-online-harassment-a-glossary-of-terms/
[63] Khoo, C. (2021). *Deplatforming misogyny: Report on platform liability for technology-facilitated gender-based violence.* Women's Legal Education and Action Fund. https://www.leaf.ca/wp-content/uploads/2021/04/Full-Report-Deplatforming-Misogyny.pdf
[64] Khoo, C. (2021). *Deplatforming misogyny: Report on platform liability for technology-facilitated gender-based violence.* Women's Legal Education and Action Fund. https://www.leaf.ca/wp-content/uploads/2021/04/Full-Report-Deplatforming-Misogyny.pdf

[65] Biros-Bolton, N. (2021). *Tech-facilitated violence*. Women's Legal Education and Action Fund (LEAF). https://www.leaf.ca/publication/tech-facilitated-violence/
[66] Elash, A. (2019). *It's time to start charging people for using stalkerware to harass their partners, watchdog group says*. CBC. https://www.cbc.ca/news/science/stalkerware-cellphone-abuse-women-citizen-lab-1.5171458
[67] Lalonde, D. (2021). Policy options on non-consensual deepnudes and sexual deepfakes. *Learning Network Brief 39.* London, Ontario: Learning Network, Centre for Research & Education on Violence Against Women & Children. https://www.vawlearningnetwork.ca/our-work/briefs/briefpdfs/Learning-Network-Brief-39.pdf
[68] Porter, C. (2021). *Toronto van attacker found guilty in city's worst mass killing*. The New York Times https://www.nytimes.com/2021/03/03/world/canada/toronto-van-alek-minassian.html
[69] Biros-Bolton, N. (2021). Tech-facilitated violence. Women's Legal Education and Action Fund (LEAF). https://www.leaf.ca/publication/tech-facilitated-violence/
[70] Khoo, C. (2021). *Deplatforming misogyny: Report on platform liability for technology-facilitated gender-based violence.* Women's Legal Education and Action Fund. https://www.leaf.ca/wp-content/uploads/2021/04/Full-Report-Deplatforming-Misogyny.pdf
[71] Judd, A. (2021). *Amanda Todd's accused cyberbully extradited to Canada to face charges.* Global News. https://globalnews.ca/news/7622978/amanda-todds-accused-cyberbully-extradited-canada/
[72] Canadian Centre for Child Protection. (2017). *Online luring*. https://www.cybertip.ca/pdfs/C3P_SafetySheet_OnlineLuring_en.pdf
[73] Rosen, K. (2021). The pandemic has caused an increase in online child luring. Here is how you can keep children safe. CTV news Winnipeg. https://winnipeg.ctvnews.ca/the-pandemic-has-caused-an-increase-in-online-child-luring-here-is-how-you-can-keep-children-safe-1.5526466
[74] Biros-Bolton, N. (2021). *Tech-facilitated violence.* Women's Legal Education and Action Fund (LEAF). https://www.leaf.ca/publication/tech-facilitated-violence/
[75] Khoo, C. (2021). *Deplatforming misogyny: Report on platform liability for technology-facilitated gender-based violence.* Women's Legal Education and Action Fund. https://www.leaf.ca/wp-content/uploads/2021/04/Full-Report-Deplatforming-Misogyny.pdf
[76] Steeves, V., & Bailey, J. (2021). *Submission to the United Nations special rapporteur on the right to privacy toward a better understanding of privacy: Children's right to privacy and autonomy.* Submission to the Special Rapporteur on the Right to Privacy. http://www.equalityproject.ca/wp-content/uploads/2021/03/Childrens-Right-to-Privacy-UN-Submission.pdf
[77] Bailey, J. & Steeves, V. (2019). *Submission to the standing committee on justice & human rights regarding online hate.* Submission Concurred in by the Canadian Women's Foundation. http://www.equalityproject.ca/wp-content/uploads/2019/05/FINAL-Bailey-Steeves-Submission-9-May-2019.pdf
[78] Canadian Centre for Child Protection. (2021). *Project Arachnid: Online availability of child sexual abuse material: An analysis of CSAM and harmful-abusive content linked to certain electronic service providers*. https://protectchildren.ca/pdfs/C3P_ProjectArachnidReport_en.pdf
[79] Bailey, J. & Mathen, C. (2019). Technology-facilitated Violence Against Women & Girls: Assessing the Canadian Criminal Law Response. *Canadian Bar Review, 97(3),* 564. https://cbr.cba.org/index.php/cbr/article/view/4562/4468
[80] Bailey, J. & Mathen, C. (2019). Technology-facilitated Violence Against Women & Girls: Assessing the Canadian Criminal Law Response. *Canadian Bar Review, 97(3),* 564. https://cbr.cba.org/index.php/cbr/article/view/4562/4468
[81] Bailey, J. & Mathen, C. (2019). Technology-facilitated Violence Against Women & Girls: Assessing the Canadian Criminal Law Response. *Canadian Bar Review, 97(3),* 564. https://cbr.cba.org/index.php/cbr/article/view/4562/4468
[82] Bailey, J. & Mathen, C. (2019). Technology-facilitated Violence Against Women & Girls: Assessing the Canadian Criminal Law Response. *Canadian Bar Review, 97(3),* 564. https://cbr.cba.org/index.php/cbr/article/view/4562/4468
[83] Bailey, J. & Mathen, C. (2019). Technology-facilitated Violence Against Women & Girls: Assessing the Canadian Criminal Law Response. *Canadian Bar Review, 97(3),* 564. https://cbr.cba.org/index.php/cbr/article/view/4562/4468
[84] Karadeglija, A. (2021). *New hate law could have chilling effect, free speech advocates say*. National Post. https://nationalpost.com/news/politics/new-hate-law-could-have-chilling-effect-free-speech-advocates-say
[85] Bailey, J. & Mathen, C. (2019). Technology-facilitated Violence Against Women & Girls: Assessing the Canadian Criminal Law Response. *Canadian Bar Review, 97(3)*, 564. https://cbr.cba.org/index.php/cbr/article/view/4562/4468
[86] Bailey, J., Steeves, V. & Dunn, S. (2017). *Submission to The special rapporteur on violence against women, Re: Regulating online violence and harassment against women.* Submission to the United Nations Special Rapporteur on

Violence Against Women. http://www.equalityproject.ca/wp-content/uploads/2017/12/Bailey-Steeves-Dunn-Submission-27-Sep-2017.pdf

[87] Canadian Women's Foundation. (2019). *Online hate: Submission to the house of commons standing committee on justice and human rights.*

[88] Bailey, J. & Steeves, V. (2019). *Submission to the standing committee on justice & human rights regarding online hate*. Submission Concurred in by the Canadian Women's Foundation. http://www.equalityproject.ca/wp-content/uploads/2019/05/FINAL-Bailey-Steeves-Submission-9-May-2019.pdf

[89] Bailey, J. & Steeves, V. (2019). *Submission to the standing committee on justice & human rights regarding online hate.* Submission Concurred in by the Canadian Women's Foundation. http://www.equalityproject.ca/wp-content/uploads/2019/05/FINAL-Bailey-Steeves-Submission-9-May-2019.pdf

[90] Bailey, J. & Steeves, V. (2019). *Submission to the standing committee on justice & human rights regarding online hate.* Submission Concurred in by the Canadian Women's Foundation. http://www.equalityproject.ca/wp-content/uploads/2019/05/FINAL-Bailey-Steeves-Submission-9-May-2019.pdf

[91] Canadian Centre for Child Protection. (2016). *Child sexual abuse images on the internet: A cybertips.ca analysis*. https://protectchildren.ca/pdfs/CTIP_CSAResearchReport_2016_en.pdf

[92] West Coast LEAF. (2014). *West Coast LEAF's submission to the standing committee on justice and human rights on bill c-13: an act to amend the criminal code, the Canada evidence act, the competition act, and the mutual legal assistance in criminal matters act.* http://www.westcoastleaf.org/wp-content/uploads/2014/11/2014-05-13-SUBMISSION-Standing-Committee-on-JHR-on-Bill-C-13.pdf

[93] Canadian Centre for Child Protection. (2021). *Project Arachnid: Online availability of child sexual abuse material: an analysis of CSAM and harmful-abusive content linked to certain electronic service providers*. https://protectchildren.ca/pdfs/C3P_ProjectArachnidReport_en.pdf

[94] Canadian Centre for Child Protection. (2019). *How we are failing children: Changing the paradigm. Framework for the protection and rights of children in the removal of child sexual abuse images and harmful/abusive images of children*. https://protectchildren.ca/pdfs/C3P_ChildRightsFramework_en.pdf

[95] Lalonde, D. (2021). Policy options on non-consensual deepnudes and sexual deepfakes. *Learning Network Brief 39.* London, Ontario: Learning Network, Centre for Research & Education on Violence Against Women & Children. https://www.vawlearningnetwork.ca/our-work/briefs/briefpdfs/Learning-Network-Brief-39.pdf

[96] West Coast LEAF. (2014*). #CyberMisogyny: Using and strengthening Canadian legal responses to gendered hate and harassment online*. http://www.westcoastleaf.org/wp-content/uploads/2014/10/2014-REPORT-CyberMisogyny.pdf

[97] Canadian Centre for Child Protection. (2021). *Project Arachnid: Online availability of child sexual abuse material: an analysis of CSAM and harmful-abusive content linked to certain electronic service providers*. https://protectchildren.ca/pdfs/C3P_ProjectArachnidReport_en.pdf

[98] Khoo, C. (2021). *Deplatforming misogyny: Report on platform liability for technology-facilitated gender-based violence.* Women's Legal Education and Action Fund. https://www.leaf.ca/wp-content/uploads/2021/04/Full-Report-Deplatforming-Misogyny.pdf

[99] Parsons, C., Molnar, A., Dalek, J., Knockel, J., Kenyon, M., Haselton, B., Khoo, C., & Deibert, R. (2019). *The predator in your pocket: A multidisciplinary assessment of the stalkerware application industry*. https://citizenlab.ca/docs/stalkerware-holistic.pdf

[100] Stevenson, M. (2019). *Technologically-facilitated violence against women and girls: The Canadian compromise.* International Human Rights Internship Program Working Paper Series, Vol. 7, No. 1. https://www.mcgill.ca/humanrights/files/humanrights/ihri_v7_2019_stevenson.pdf.9_stevenson.pdf

[101] Fairbairn, J., Bivens, R., & Dawson, M. (2013). *Sexual violence and social media: building a framework for prevention*. https://www.octevaw-cocvff.ca/s/sexual-violence-and-social-media.pdf

[102] Khoo, C. (2021). *Deplatforming misogyny: Report on platform liability for technology-facilitated gender-based violence*. Women's Legal Education and Action Fund. https://www.leaf.ca/wp-content/uploads/2021/04/Full-Report-Deplatforming-Misogyny.pdf

[103] Khoo, C., Robertson, K., & Deibert, R. (2019). *Installing fear: A Canadian legal and policy analysis of using, developing, and selling smartphone spyware and stalkerware applications.* https://citizenlab.ca/docs/stalkerware-legal.pdf

[104] Parsons, C., Molnar, A., Dalek, J., Knockel, J., Kenyon, M., Haselton, B., Khoo, C., & Deibert, R. (2019). *The predator in your pocket: A multidisciplinary assessment of the stalkerware application industry*. https://citizenlab.ca/docs/stalkerware-holistic.pdf

[105] Steeves, V., & Bailey, J. (2021). *Submission to the United Nations special rapporteur on the right to privacy toward a better understanding of privacy: Children's right to privacy and autonomy*. Submission to the Special Rapporteur on the Right to Privacy. http://www.equalityproject.ca/wp-content/uploads/2021/03/Childrens-Right-to-Privacy-UN-Submission.pdf
[106] Bailey, J. & Steeves, V. (2019). *Submission to the standing committee on justice & human rights regarding online hate.* Submission Concurred in by the Canadian Women's Foundation. http://www.equalityproject.ca/wp-content/uploads/2019/05/FINAL-Bailey-Steeves-Submission-9-May-2019.pdf
[107] Steeves, V. (2020). *Taking online rights seriously: Ensuring children's active participation in networked spaces, submission to the 5th/6th review of children's rights in Canada (Convention on the rights of the child)*. http://www.equalityproject.ca/wp-content/uploads/2020/03/eQuality-Project-Report-on-CRC-Canada-State-Report.pdf
[108] Steeves, V. (2020). Taking online rights seriously: Ensuring children's active participation in networked spaces, submission to the 5th/6th review of children's rights in Canada (Convention on the Rights of the Child). http://www.equalityproject.ca/wp-content/uploads/2020/03/eQuality-Project-Report-on-CRC-Canada-State-Report.pdf
[109] Khoo, C. (2021). *Deplatforming misogyny: Report on platform liability for technology-facilitated gender-based violence*. Women's Legal Education and Action Fund. https://www.leaf.ca/wp-content/uploads/2021/04/Full-Report-Deplatforming-Misogyny.pdf
[110] West Coast LEAF. (2014*). #CyberMisogyny: Using and strengthening Canadian legal responses to gendered hate and harassment online*. http://www.westcoastleaf.org/wp-content/uploads/2014/10/2014-REPORT-CyberMisogyny.pdf
[111] West Coast LEAF. (2014). *#CyberMisogyny: Using and strengthening Canadian legal responses to gendered hate and harassment online.* http://www.westcoastleaf.org/wp-content/uploads/2014/10/2014-REPORT-CyberMisogyny.pdf
[112] West Coast LEAF. (2014). *#CyberMisogyny: Using and strengthening Canadian legal responses to gendered hate and harassment online*. http://www.westcoastleaf.org/wp-content/uploads/2014/10/2014-REPORT-CyberMisogyny.pdf
[113] Canadian Centre for Child Protection. (2021). *Project Arachnid: Online availability of child sexual abuse material: An analysis of CSAM and harmful-abusive content linked to certain electronic service providers*. https://protectchildren.ca/pdfs/C3P_ProjectArachnidReport_en.pdf
[114] Stevenson, M. (2019). *Technologically-facilitated violence against women and girls: The Canadian compromise.* International Human Rights Internship Program Working Paper Series, Vol. 7, No. 1. https://www.mcgill.ca/humanrights/files/humanrights/ihri_v7_2019_stevenson.pdf
[115] Khoo, C., Robertson, K., & Deibert, R. (2019). Installing Fear: A Canadian Legal and Policy Analysis of Using, Developing, and Selling Smartphone Spyware and Stalkerware Applications: https://citizenlab.ca/docs/stalkerware-legal.pdf
[116] Canadian Women's Foundation. (2019). *Online Hate: Submission to the house of commons standing committee on justice and human rights.*
[117] Deibert, R. J. (2017). *Submission of the Citizen Lab (Munk School of Global Affairs, University of Toronto) to the United Nations special rapporteur on violence against women, its causes and consequences, Ms. Dubravka Šimonović.* https://citizenlab.ca/wp-content/uploads/2017/11/Final-UNSRVAG-CitizenLab.pdf
[118] Liliefeldt. R. (2018). *How cyberviolence is threatening and silencing women*. Policy Options. https://policyoptions.irpp.org/magazines/june-2018/how-cyberviolence-is-threatening-and-silencing-women/
[119] West Coast LEAF. (2014). *#CyberMisogyny: Using and strengthening Canadian legal responses to gendered hate and harassment online.* http://www.westcoastleaf.org/wp-content/uploads/2014/10/2014-REPORT-CyberMisogyny.pdf
[120] West Coast LEAF. (2014). *#CyberMisogyny: Using and strengthening Canadian legal responses to gendered hate and harassment online*. http://www.westcoastleaf.org/wp-content/uploads/2014/10/2014-REPORT-CyberMisogyny.pdf
[121] Parsons, C., Molnar, A., Dalek, J., Knockel, J., Kenyon, M., Haselton, B., Khoo, C., & Deibert, R. (2019). *The predator in your pocket: A multidisciplinary assessment of the stalkerware application industry.* https://citizenlab.ca/docs/stalkerware-holistic.pdf
[122] Parsons, C., Molnar, A., Dalek, J., Knockel, J., Kenyon, M., Haselton, B., Khoo, C., & Deibert, R. (2019). *The predator in your pocket: A multidisciplinary assessment of the stalkerware application industry*. https://citizenlab.ca/docs/stalkerware-holistic.pdf
[123] YWCA. (2015). *PROJECT SHIFT: Creating a safer digital world for young women. Needs assessment report summary.* https://ywcacanada.ca/wp-content/uploads/2019/05/Project-Shift_Needs-Assessment-Report-Summary.pdf
[124] Khoo, C. (2021). *Deplatforming misogyny: Report on platform liability for technology-facilitated gender-based violence*. Women's Legal Education and Action Fund. https://www.leaf.ca/wp-content/uploads/2021/04/Full-Report-Deplatforming-Misogyny.pdf

[125] West Coast LEAF. (2014). *West Coast LEAF's submission to the standing committee on justice and human rights on bill c-13: an act to amend the criminal code, the Canada evidence act, the competition act, and the mutual legal assistance in criminal matters act*. http://www.westcoastleaf.org/wp-content/uploads/2014/11/2014-05-13-SUBMISSION-Standing-Committee-on-JHR-on-Bill-C-13.pdf
[126] Public Policy Forum. (2021). *Final Report 2020-2021 - Canadian commission on democratic expression: harms reduction: a six-step program to protect democratic expression online*. https://ppforum.ca/wp-content/uploads/2021/01/CanadianCommissionOnDemocraticExpression-PPF-JAN2021-EN.pdf
[127] Furrie, A. D., Lero, D. S., D'Aubin, A., and Ewles, G. (2016). *Willing but unable: A population in waiting*. Centre for Research on Work Disability Policy. https://www.crwdp.ca/sites/default/files/Research%20and%20Publications/finalwilling_but_unable_kp_final.pdf
[128] Cuiker, W. (2020). *Inclusive innovation: Using technology to bridge the urban-rural divide*. Public Policy Forum. https://www.ryerson.ca/diversity/reports/Inclusive-Innovation-Using-Technology-to-Bridge-the-Urban-Rural-Divide-PPF-JAN2019-EN.pdf
[129] Canadian Rural Revitalization Foundation. (2021). *CRRF's submission to infrastructure Canada's building the Canada we want in 2050 consultation*. http://crrf.ca/building-the-canada-we-want-in-2050/
[130] Bramwell, A., Coates, K., and Bradford, N. (2019). *Expanding digital opportunity in canada? digital inclusion and intelligent communities*. ON: Innovation Policy Lab, Munk School of Global Affairs & Public Policy. https://munkschool.utoronto.ca/ipl/creating-digital-opportunity/
[131] Cuiker, W. (2020). *Inclusive innovation: Using technology to bridge the urban-rural divide*. Public Policy Forum. https://www.ryerson.ca/diversity/reports/Inclusive-Innovation-Using-Technology-to-Bridge-the-Urban-Rural-Divide-PPF-JAN2019-EN.pdf
[132] Council of Canadian Academics. (2021). *Waiting to connect: The expert panel on high-throughput networks for rural and remote communities in Canada*. Ontario. https://cca-reports.ca/wp-content/uploads/2021/10/Waiting-to-Connect_FINAL-EN_digital.pdf
[133] Pearson, M. (2017). *Rural broadband: Policy recommendations for improving broadband access and adoption in rural Alberta*. Alberta Centre for Sustainable Rural Communities. https://www.ualberta.ca/augustana/media-library/research/acsrc/policy-briefs/rural-broadband-policy-brief.pdf
[134] Council of Canadian Academics. (2021). *Waiting to connect: The expert panel on high-throughput networks for rural and remote communities in Canada*. Ontario. https://cca-reports.ca/wp-content/uploads/2021/10/Waiting-to-Connect_FINAL-EN_digital.pdf
[135] Cuiker, W. (2020). *Inclusive innovation: Using technology to bridge the urban-rural divide*. Public Policy Forum. https://www.ryerson.ca/diversity/reports/Inclusive-Innovation-Using-Technology-to-Bridge-the-Urban-Rural-Divide-PPF-JAN2019-EN.pdf
[136] Inclusion Canada. (2021). *Position on financial security and income support*. https://inclusioncanada.ca/wp-content/uploads/2021/07/Jul21-Position-Income-Security-2021_Final_May-11.pdf
[137] Van Berkum, A. and Oudshoorn, A. (2015). Best practice guideline for ending women's and girl's homelessness. https://www.abeoudshoorn.com/wp-content/uploads/2015/08/Best-Practice-Guideline-for-Ending-Womens-and-Girls-Homelessness.pdf
[138] Disability and Work in Canada Steering Committee. (2019). *Moving forward together: A Pan-Canadian strategy for disability and work*. https://www.crwdp.ca/sites/default/files/dwc_strategy_-_moving_forward_together.pdf
[139] Stevenson, M. (2019). *Technologically-facilitated violence against women and girls: The Canadian compromise.* International Human Rights Internship Program Working Paper Series, Vol. 7, No. 1. https://www.mcgill.ca/humanrights/files/humanrights/ihri_v7_2019_stevenson.pdf.
[140] AGE-WELL. (2020). *AGE-WELL position paper on mobile technology and data-informed approaches for healthy aging and aging-in-place*. https://agewell-nce.ca/wp-content/uploads/2017/11/Mobile-technology-and-data-informed-approaches-WP7.3.pdf
[141] Social Research and Demonstration Corporation. (2017). *Assistive equipment and technology*. https://www.srdc.org/media/200068/at-final-report.pdf
[142] Bartlett, L. and Smith Fowler, H. (2019). *A Canadian roadmap for an aging society: current trends, opportunities and implications for standards*. Social Research and Demonstration Corporation. https://www.csagroup.org/wp-content/uploads/CSA-Group-Research-Aging-Society-Standard-Roadmap.pdf
[143] Social Research and Demonstration Corporation. (2017). *Assistive equipment and technology*. https://www.srdc.org/media/200068/at-final-report.pdf

[144] Furrie, A. D., Lero, D. S., D'Aubin, A., and Ewles, G. (2016). *Willing but unable: A population in waiting*. Centre for Research on Work Disability Policy. https://www.crwdp.ca/sites/default/files/Research%20and%20Publications/finalwilling_but_unable_kp_final.pdf
[145] Social Research and Demonstration Corporation. (2017). *Assistive equipment and technology*. https://www.srdc.org/media/200068/at-final-report.pdf
[146] Dawson, M. (2021). *Not the 'Golden Years': Femicide of older women in Canada*. https://www.victimsfirst.gc.ca/res/cor/FOW-FOW/FEMICIDE%20OF%20OLDER%20WOMEN_FINAL_April%2027,%202021.pdf
[147] National Institute on Ageing. (2020). *An evidence informed national seniors strategy for Canada - third edition*. Toronto, ON: National Institute on Ageing. http://nationalseniorsstrategy.ca/wp-content/uploads/2020/09/NSS_2020_Third_Edition.pdf
[148] National Institute on Ageing. (2020). *An evidence informed national seniors strategy for Canada - third edition*. Toronto, ON: National Institute on Ageing: http://nationalseniorsstrategy.ca/wp-content/uploads/2020/09/NSS_2020_Third_Edition.pdf
[149] Van Berkum, A. and Oudshoorn, A. (2015). *Best practice guideline for ending women's and girl's homelessness*. https://www.abeoudshoorn.com/wp-content/uploads/2015/08/Best-Practice-Guideline-for-Ending-Womens-and-Girls-Homelessness.pdf
[150] Lane, J., and Pittman, S. (2020). *Towards a rural digital economic strategy*. Canada West Foundation. https://cwf.ca/wp-content/uploads/2020/07/2020-07-CWF_Upgrade_Digital_Economy_Report.pdf
[151]Canadian Rural Revitalization Foundation. (2020). *Gender-based violence in rural and remote communities – Impacts from Covid-19*. Rural Insights Series: Covid-19. http://crrf.ca/ri-genderbasedviolence/
[152] Stevenson, M. (2019). *Technologically-facilitated violence against women and girls: The Canadian compromise.* International Human Rights Internship Program Working Paper Series, Vol. 7, No. 1. https://www.mcgill.ca/humanrights/files/humanrights/ihri_v7_2019_stevenson.pdf
[153] Stevenson, M. (2019). *Technologically-facilitated violence against women and girls: The Canadian compromise.* International Human Rights Internship Program Working Paper Series, Vol. 7, No. 1. https://www.mcgill.ca/humanrights/files/humanrights/ihri_v7_2019_stevenson.pdf.
[154] YWCA. (2015). *PROJECT SHIFT: Creating a safer digital world for young women. needs assessment report summary.* https://ywcacanada.ca/wp-content/uploads/2019/05/Project-Shift_Needs-Assessment-Report-Summary.pdf
[155] Canadian Women's Foundation. (2019). *Online hate: Submission to the house of commons standing committee on justice and human rights.*
[156] Stevenson, M. (2019). *Technologically-facilitated violence against women and girls: The Canadian compromise.* International Human Rights Internship Program Working Paper Series, Vol. 7, No. 1. https://www.mcgill.ca/humanrights/files/humanrights/ihri_v7_2019_stevenson.pdf.
[157] Khoo, C. (2021). *Deplatforming misogyny: Report on platform liability for technology-facilitated gender-based violence.* Women's Legal Education and Action Fund. https://www.leaf.ca/wp-content/uploads/2021/04/Full-Report-Deplatforming-Misogyny.pdf
[158] Deibert, R. J. (2017). *Submission of the Citizen Lab (Munk School of Global Affairs, University of Toronto) to the United Nations special rapporteur on violence against women, its causes and consequences, Ms. Dubravka Šimonović.* https://citizenlab.ca/wp-content/uploads/2017/11/Final-UNSRVAG-CitizenLab.pdf
[159] Canadian Centre for Child Protection. (2016). *Child sexual abuse images on the internet: A Cybertips.ca analysis.* https://protectchildren.ca/pdfs/CTIP_CSAResearchReport_2016_en.pdf
[160] Khoo, C. (2021). *Deplatforming misogyny: Report on platform liability for technology-facilitated gender-based violence*. Women's Legal Education and Action Fund. https://www.leaf.ca/wp-content/uploads/2021/04/Full-Report-Deplatforming-Misogyny.pdf
[161] Biros-Bolton, N. (2021). *Tech-facilitated Violence: The elements and impact of online gender-based hatred and oppression.* Women's Legal Education and Action Fund. https://www.leaf.ca/publication/tech-facilitated-violence/
[162] Deibert, R. J. (2017). *Submission of the Citizen Lab (Munk School of Global Affairs, University of Toronto) to the United Nations special rapporteur on violence against women, its causes and consequences, Ms. Dubravka Šimonović*. https://citizenlab.ca/wp-content/uploads/2017/11/Final-UNSRVAG-CitizenLab.pdf
[163] Ottawa Coalition to End Violence Against Women. (n.d.) *Tech without violence prevention framework.* https://www.techwithoutviolence.ca/tech-without-violence-prevention-framework
164 Deibert, R. J. (2017). *Submission of the Citizen Lab (Munk School of Global Affairs, University of Toronto) to the*

United Nations special rapporteur on violence against women, its causes and consequences, Ms. Dubravka Šimonović. https://citizenlab.ca/wp-content/uploads/2017/11/Final-UNSRVAG-CitizenLab.pdf

[165] Stevenson, M. (2019). *Technologically-facilitated violence against women and girls: The Canadian compromise*. International Human Rights Internship Program Working Paper Series, Vol. 7, No. 1. https://www.mcgill.ca/humanrights/files/humanrights/ihri_v7_2019_stevenson.pdf

[166] Ottawa Coalition to End Violence Against Women. (n.d.) *Tech without violence prevention framework.* https://www.techwithoutviolence.ca/tech-without-violence-prevention-framework

[167] Ottawa Coalition to End Violence Against Women. (n.d.) *Tech without violence prevention framework.* https://www.techwithoutviolence.ca/tech-without-violence-prevention-framework

[168] Liliefeldt. R. (2018). *How Cyberviolence is Threatening and Silencing Women*. *Policy Options.* https://policyoptions.irpp.org/magazines/june-2018/how-cyberviolence-is-threatening-and-silencing-women/

[169] Canadian Centre for Child Protection. (2021). *Project Arachnid: Online availability of child sexual abuse material: an analysis of CSAM and harmful-abusive content linked to certain electronic service providers.* https://protectchildren.ca/pdfs/C3P_ProjectArachnidReport_en.pdf

[170] Canadian Centre for Child Protection. (2021). *Project Arachnid: Online availability of child sexual abuse material: an analysis of csam and harmful-abusive content linked to certain electronic service providers*. https://protectchildren.ca/pdfs/C3P_ProjectArachnidReport_en.pdf

[171] Canadian Centre for Child Protection. (2021). *Project Arachnid: Online availability of child sexual abuse material: an analysis of CSAM and harmful-abusive content linked to certain electronic service providers.* https://protectchildren.ca/pdfs/C3P_ProjectArachnidReport_en.pdf

[172] Canadian Centre for Child Protection. (2021). *Project Arachnid: Online availability of child sexual abuse material: an analysis of CSAM and harmful-abusive content linked to certain electronic service providers.* https://protectchildren.ca/pdfs/C3P_ProjectArachnidReport_en.pdf

[173] Canadian Centre for Child Protection. (2021). *Project Arachnid: Online availability of child sexual abuse material: an analysis of CSAM and harmful-abusive content linked to certain electronic service providers.* https://protectchildren.ca/pdfs/C3P_ProjectArachnidReport_en.pdf

[174] Public Policy Forum. (2021). *Final Report 2020-2021 - Canadian commission on democratic expression: Harms reduction: A six-step program to protect democratic expression online*. https://ppforum.ca/wp-content/uploads/2021/01/CanadianCommissionOnDemocraticExpression-PPF-JAN2021-EN.pdf

[175] Khoo, C. (2021). *Deplatforming misogyny: Report on platform liability for technology-facilitated gender-based violence.* Women's Legal Education and Action Fund. https://www.leaf.ca/wp-content/uploads/2021/04/Full-Report-Deplatforming-Misogyny.pdf

[176] Parsons, C., Molnar, A., Dalek, J., Knockel, J., Kenyon, M., Haselton, B., Khoo, C., & Deibert, R. (2019). *The predator in your pocket: A multidisciplinary assessment of the stalkerware application industry.* https://citizenlab.ca/docs/stalkerware-holistic.pdf

[177] Khoo, C., Robertson, K., & Deibert, R. (2019). *Installing fear: A Canadian legal and policy analysis of using, developing, and selling smartphone spyware and stalkerware applications*. https://citizenlab.ca/docs/stalkerware-legal.pdf

[178] Ottawa Coalition to End Violence Against Women. (n.d.) *Dating apps without violence.* https://www.techwithoutviolence.ca/dating-apps-without-violence

[179] Deibert, R. J. (2017). *Submission of the Citizen Lab (Munk School of Global Affairs, University of Toronto) to the United Nations special rapporteur on violence against women, its causes and consequences, Ms. Dubravka Šimonović.* https://citizenlab.ca/wp-content/uploads/2017/11/Final-UNSRVAG-CitizenLab.pdf

[180] Khoo, C. (2021). *Deplatforming misogyny: Report on platform liability for technology-facilitated gender-based violence*. Women's Legal Education and Action Fund. https://www.leaf.ca/wp-content/uploads/2021/04/Full-Report-Deplatforming-Misogyny.pdf

[181] Khoo, C. (2021). *Deplatforming misogyny: Report on platform liability for technology-facilitated gender-based violence*. Women's Legal Education and Action Fund. https://www.leaf.ca/wp-content/uploads/2021/04/Full-Report-Deplatforming-Misogyny.pdf

[182] Public Policy Forum. (2021). *Final report 2020-2021 - Canadian commission on democratic expression: Harms reduction: A six-step program to protect democratic expression online*. https://ppforum.ca/wp-content/uploads/2021/01/CanadianCommissionOnDemocraticExpression-PPF-JAN2021-EN.pdf

[183] West Coast LEAF. (2014). *West Coast LEAF's submission to the standing committee on justice and human rights on Bill C-13: An act to amend the criminal code, the Canada evidence act, the competition act, and the mutual legal assistance*

in criminal matters act. http://www.westcoastleaf.org/wp-content/uploads/2014/11/2014-05-13-SUBMISSION-Standing-Committee-on-JHR-on-Bill-C-13.pdf
[184] YWCA. (2015). *PROJECT SHIFT: Creating a safer digital world for young women. Needs assessment report summary*. https://ywcacanada.ca/wp-content/uploads/2019/05/Project-Shift_Needs-Assessment-Report-Summary.pdf
[185] YWCA. (2015). *PROJECT SHIFT: Creating a safer digital world for young women. Needs assessment report summary*. https://ywcacanada.ca/wp-content/uploads/2019/05/Project-Shift_Needs-Assessment-Report-Summary.pdf
[186] Fairbairn, J., Bivens, R., & Dawson, M. (2013). *Sexual violence and social media: Building a framework for prevention.* https://www.octevaw-cocvff.ca/s/sexual-violence-and-social-media.pdf
[187] YWCA. (2015). *PROJECT SHIFT: Creating a safer digital world for young women. Needs assessment report summary*. https://ywcacanada.ca/wp-content/uploads/2019/05/Project-Shift_Needs-Assessment-Report-Summary.pdf
[188] Canadian Centre for Child Protection. (2016). *Child sexual abuse images on the internet: A cybertips.ca analysis*. https://protectchildren.ca/pdfs/CTIP_CSAResearchReport_2016_en.pdf
[189] Dunn, S. (2020). *Technology-facilitated gender-based violence: an overview*. Supporting a Safer Internet Paper No. 1. Centre for International Governance Innovation. https://www.cigionline.org/static/documents/documents/SaferInternet_Paper%20no%201_0.pdf
[190] Stevenson, M. (2019). *Technologically-facilitated violence against women and girls: The Canadian compromise.* International Human Rights Internship Program Working Paper Series, Vol. 7, No. 1. https://www.mcgill.ca/humanrights/files/humanrights/ihri_v7_2019_stevenson.pdf.
[191] Dunn, S. (2020). *Technology-facilitated gender-based violence: An overview*. Supporting a Safer Internet Paper No. 1, Centre for International Governance Innovation. https://www.cigionline.org/static/documents/documents/SaferInternet_Paper%20no%201_0.pdf
[192] YWCA. (2015). *PROJECT SHIFT: Creating a safer digital world for young women. Needs assessment report summary.* https://ywcacanada.ca/wp-content/uploads/2019/05/Project-Shift_Needs-Assessment-Report-Summary.pdf
[193] Canadian Centre for Child Protection. (2019). *How we are failing children: Changing the paradigm. Framework for the protection and rights of children in the removal of child sexual abuse images and harmful/abusive images of children*. https://protectchildren.ca/pdfs/C3P_ChildRightsFramework_en.pdf
[194] Liliefeldt. R. (2018). *How cyberviolence is threatening and silencing women.* Policy Options. https://policyoptions.irpp.org/magazines/june-2018/how-cyberviolence-is-threatening-and-silencing-women/
[195] Brisson-Boivin, K. (2019). *Young Canadians pushing back against hate online*. Ottawa: MediaSmarts. https://mediasmarts.ca/sites/mediasmarts/files/publication-report/full/young-canadians-online-hate.pdf
[196] Fairbairn, J., Bivens, R., & Dawson, M. (2013). *Sexual violence and social media: Building a framework for prevention*. https://www.octevaw-cocvff.ca/s/sexual-violence-and-social-media.pdf
[197] Stevenson, M. (2019). *Technologically-facilitated violence against women and girls: The Canadian compromise*. International Human Rights Internship Program Working Paper Series, Vol. 7, No. 1. https://www.mcgill.ca/humanrights/files/humanrights/ihri_v7_2019_stevenson.pdf
[198] Liliefeldt. R. (2018). *How cyberviolence is threatening and silencing women*. Policy Options: https://policyoptions.irpp.org/magazines/june-2018/how-cyberviolence-is-threatening-and-silencing-women/
[199] Stevenson, M. (2019). *Technologically-facilitated violence against women and girls: The Canadian compromise*. International Human Rights Internship Program Working Paper Series, Vol. 7, No. 1. https://www.mcgill.ca/humanrights/files/humanrights/ihri_v7_2019_stevenson.pdf
[200] YWCA. (2015). *PROJECT SHIFT: Creating a safer digital world for young women. Needs assessment report summary.* https://ywcacanada.ca/wp-content/uploads/2019/05/Project-Shift_Needs-Assessment-Report-Summary.pdf
[201] West Coast LEAF. (2014). *#CyberMisogyny: Using and strengthening Canadian legal responses to gendered hate and harassment online*. http://www.westcoastleaf.org/wp-content/uploads/2014/10/2014-REPORT-CyberMisogyny.pdf
[202] Stevenson, M. (2019). *Technologically-facilitated violence against women and girls: The Canadian compromise.* International Human Rights Internship Program Working Paper Series, Vol. 7, No. 1. https://www.mcgill.ca/humanrights/files/humanrights/ihri_v7_2019_stevenson.pdf
[203] Stevenson, M. (2019). *Technologically-facilitated violence against women and girls: The Canadian compromise*. International Human Rights Internship Program Working Paper Series, Vol. 7, No. 1. https://www.mcgill.ca/humanrights/files/humanrights/ihri_v7_2019_stevenson.pdf
[204] Dunn, S. (2020). *Technology-facilitated gender-based violence: An overview*. Supporting a Safer Internet Paper No. 1, Centre for International Governance Innovation. https://www.cigionline.org/static/documents/documents/SaferInternet_Paper%20no%201_0.pdf

[205] West, J. (2014). *Cyber-violence against women.* Battered Women's Support Services. https://www.bwss.org/wp-content/uploads/2014/05/CyberVAWReportJessicaWest.pdf
[206] Dunn, S. (2020). *Technology-facilitated gender-based violence: An overview*. Supporting a Safer Internet Paper No. 1, Centre for International Governance Innovation. https://www.cigionline.org/static/documents/documents/SaferInternet_Paper%20no%201_0.pdf
[207] UK Government. (2022). *Guidance: Understanding and identifying radicalisation risk in your education setting*. https://www.gov.uk/government/publications/the-prevent-duty-safeguarding-learners-vulnerable-to-radicalisation/understanding-and-identifying-radicalisation-risk-in-your-education-setting
[208] West, J. (2014). Cyber-violence against women. Battered Women's Support Services. https://www.bwss.org/wp-content/uploads/2014/05/CyberVAWReportJessicaWest.pdf
[209] Deibert, R. J. (2017). *Submission of the Citizen Lab (Munk School of Global Affairs, University of Toronto) to the United Nations special rapporteur on violence against women, its causes and consequences, Ms. Dubravka Šimonović*. https://citizenlab.ca/wp-content/uploads/2017/11/Final-UNSRVAG-CitizenLab.pdf
[210] YWCA. (2015). *PROJECT SHIFT: Creating a safer digital world for young women. Needs assessment report summary*. https://ywcacanada.ca/wp-content/uploads/2019/05/Project-Shift_Needs-Assessment-Report-Summary.pdf
[211] Equal Press. (2020). *Reporting on gender-based violence: A guide for journalists.* http://equalpress.ca/wp-content/uploads/2020/02/EP_Guidebook.pdf
[212] Deibert, R. J. (2017). *Submission of the Citizen Lab (Munk School of Global Affairs, University of Toronto) to the United Nations special rapporteur on violence against women, its causes and consequences, Ms. Dubravka Šimonović.* https://citizenlab.ca/wp-content/uploads/2017/11/Final-UNSRVAG-CitizenLab.pdf
[213] YWCA. (2015). *PROJECT SHIFT: Creating a safer digital world for young women. Needs assessment report summary*. https://ywcacanada.ca/wp-content/uploads/2019/05/Project-Shift_Needs-Assessment-Report-Summary.pdf
[214] Furrie, A. D., Lero, D. S., D'Aubin, A., and Ewles, G. (2016). *Willing but unable: A population in waiting*. Centre for Research on Work Disability Policy. https://www.crwdp.ca/sites/default/files/Research%20and%20Publications/finalwilling_but_unable_kp_final.pdf
[215] Van Berkum, A. and Oudshoorn, A. (2015). *Best practice guideline for ending women's and girl's homelessness.* https://www.abeoudshoorn.com/wp-content/uploads/2015/08/Best-Practice-Guideline-for-Ending-Womens-and-Girls-Homelessness.pdf
[216] Canadian Women's Foundation. (2019). *Online hate: Submission to the house of commons standing committee on justice and human rights.*
[217] Canadian Centre for Child Protection. (2016). *Child sexual abuse images on the internet: A Cybertips.ca analysis*. https://protectchildren.ca/pdfs/CTIP_CSAResearchReport_2016_en.pdf
[218] Canadian Centre for Child Protection. (2016). *Child sexual abuse images on the internet: A Cybertips.ca analysis.* https://protectchildren.ca/pdfs/CTIP_CSAResearchReport_2016_en.pdf
[219] YWCA. (2015). *PROJECT SHIFT: Creating a safer digital world for young women. Needs assessment report summary: https://ywcacanada.ca/wp-content/uploads/2019/05/Project-Shift_Needs-Assessment-Report-Summary.pdf*
[220] Fairbairn, J., Bivens, R., & Dawson, M. (2013). *Sexual violence and social media: Building a framework for prevention.* https://www.octevaw-cocvff.ca/s/sexual-violence-and-social-media.pdf
[221] Stevenson, M. (2019). *Technologically-facilitated violence against women and girls: The Canadian compromise.* International Human Rights Internship Program Working Paper Series, Vol. 7, No. 1. https://www.mcgill.ca/humanrights/files/humanrights/ihri_v7_2019_stevenson.pdf
[222] Dunn, S. (2020). *Technology-facilitated gender-based violence: An overview*. Supporting a Safer Internet Paper No. 1, Centre for International Governance Innovation. https://www.cigionline.org/static/documents/documents/SaferInternet_Paper%20no%201_0.pdf