

Submission to The Special Rapporteur on Violence Against Women
Re: Regulating Online Violence and Harassment Against Women

By Jane Bailey, Valerie Steeves, Suzanne Dunn
University of Ottawa
Ottawa, Canada

This submission consists of five parts:

- Part I introduces the authors and their research, and discusses terminology and research relating to technologically facilitated violence against women and girls (TFVAWG).
- Part II provides highlights of Canadian legislative models and criminal law jurisprudence relating to TFVAWG.
- Part III provides an overview of service provider responses and highlights some areas of concern.
- Part IV emphasizes the need for proactive community-based responses and highlights a few Canadian examples.
- Part V sets out our conclusions and recommendations.

I. INTRODUCTION

- 1) ***About the authors*** - All of the authors are affiliated with the University of Ottawa and with The eQuality Project, a 7-year initiative funded by a Social Sciences and Humanities Research Council of Canada (SSHRC) Partnership Grant. The eQuality Project focuses on how online behavioural profiling contributes to an environment that sets young people from vulnerable communities up for harassment, conflict and violence. Professors Bailey and Steeves co-lead The eQuality Project, while Suzanne Dunn (a University of Ottawa PhD student in Law, whose LLM research paper focused on image-based abuse) is funded by a Project bursary. Additionally, Professors Bailey and Steeves previously co-led The eGirls Project, a 3-year initiative funded by a SSHRC Partnership Development Grant, which focused on girls' and young women's experiences relating to privacy, equality and gender performance on social media. Outcomes from The eGirls Project interviews with girls and young women, including in relation to harassment carried out online, were published in an edited collection called *eGirls, eCitizens* (Bailey and Steeves, 2015).¹
- 2) ***TFVAWG from a human rights perspective*** - Our past and ongoing work leads us to approach TFVAWG from a human rights perspective. TFVAWG can be perpetrated in a variety of forms, including threats; repeated, unwanted and harassing communications; unauthorized distribution of intimate images; impersonation; unauthorized disclosure of personal

¹ *eGirls, eCitizens* is available for free download here: <
<https://press.uottawa.ca/egirls-ecitizens.html>>.

information; and the sexual trafficking of women and girls (Bailey and Mathen, 2017). It can lead to fear, social withdrawal, physical and psychological illness, physical danger and harm, serious consequences relating to reputation that affect targets' social, employment and family lives, and, in limited circumstances can be a contributing factor to self-harming behaviours and suicide (West, 2014 at 17-20). As a result, TFVAWG affects women's and girls' physical, sexual and psychological integrity, equality, privacy, and autonomy in ways that undermine their right to full public participation. It therefore triggers international obligations relating to both *violence*² and *discrimination*³ against women and girls.

- 3) ***Terminology: why "TFVAWG" and not "cyberbullying"?*** - In this submission, we use the term TFVAWG rather than "cyberbullying" for two reasons. First, we want to ensure that the structural underpinnings of violence facilitated against women and girls through digital technologies is not obscured or minimized by a term often associated with disagreements among individual school children. Second, we want to move away from the notion of separate online and offline spheres because this increasingly does not comport with the lived realities of most people and certainly does not comport with the lives of young Canadians. Further, conceiving of separate spheres too often leads to unrealistic and paternalistic advice that targeted women and girls should just "go offline" to avoid violence, which in many ways emulates the all-too-familiar victim-blaming approaches to VAWG that shift responsibility away from perpetrators and the community, toward survivors themselves.
- 4) ***Technologically facilitated attacks: who is targeted*** - Given the breadth of activities that could be classified as involving technologically facilitated violence, it is difficult to generalize about who is most likely to be targeted overall. However, recent research indicates that the victims of violent incidents of reported cybercrime in Canada were more likely to be female,

² The UN Declaration on the Elimination of Violence Against Women, Article 2, defines violence against women to include "physical, sexual and psychological violence occurring in the family ... within the general community ... and perpetrated or condoned by the State, wherever it occurs."

³ CEDAW, Article 1, defines discrimination against women as "... any distinction, exclusion or restriction made on the basis of sex which has the effect or purpose of impairing or nullifying the recognition, enjoyment or exercise by women, irrespective of their marital status, on a basis of equality of men and women, of human rights and fundamental freedoms in the political, economic, social, cultural, civil or any other field." The UN Convention on the Rights of the Child requires signatory states to respect and ensure the rights of all children "without discrimination of any kind" (Article 2). This includes children's right to access all forms of media "aimed at the promotion of [the child's] social, spiritual and moral well-being and physical and mental health" (Article 17). UNICEF has explicitly applied this to online media (UNICEF, 1999).

while the majority of accused were men (Mazowita and Vézina, 2014). Similarly, the Young Canadians in a Wired World study found that boys are more likely than girls to be mean or cruel online and girls are more likely to find mean or cruel comments or threats online to be a problem (Steeves, 2014 at 3-4). Being young, being a member of the LGBTQ community, and having past experiences with assault and discrimination also appear to be factors that escalate exposure to “cyberstalking” and “cyberbullying” (Government of Canada, 2016). As such, women and girls situated at vulnerable social locations may be at increased risk of TFVAWG, just as they are at increased risk of violence in general (Canadian Women’s Foundation, 2014). Further, research in the United States and Australia indicates that women are more at risk of sexualized forms of attack, such as non-consensual disclosure of intimate images, than are men (Cyber Civil Rights Initiative, 2014; Powell and Henry, 2015).

- 5) ***Environmental factors shaping TFVAWG*** – The girls and young women interviewed for The eGirls Project described a seamless integration between what once may have been thought of as “online” and “offline” experiences. While most wanted to participate online, their free and equal participation was compromised by a number of factors. These included fear of being attacked for failing to follow mediatized stereotypes of female beauty and sexuality (or for following them too closely), the risk of reputational ruin that could ensue from sexualized self-representations, and the inability to adequately control access to their information due to the privacy-invasive architecture of the online environments in which they interacted. Some stressed the need to move beyond responses to online attacks that focused on telling girls what to do and what not to do. Instead they suggested it was essential to address the underlying structural causes that disproportionately expose women and girls to attacks, such as misogyny, racism and homophobia, as well as looking more closely at the role industry played in shaping the online environment in ways that opened them up to conflict and harassment (Bailey, 2015). Research funded by Status of Women Canada and undertaken by the Ottawa Coalition to End Violence Against Women (OCTEVAW) and by YWCA Canada also demonstrated girls’ and young women’s concerns with industry practices, including complicated user agreements, and a lack of transparency in online reporting procedures and outcomes (Fairbairn and Black, 2015 at 39-40; Estable and Meyer, 2015 at 18).
- 6) ***A broad spectrum of responses is essential*** - Given the breadth of environmental factors and structural barriers at play in shaping TFVAWG, a broad spectrum, multi-pronged response is essential. While offering a range of legal recourse to those targeted should be one component of that response (along with appropriate education of and resources for judges and law enforcement agents who will be involved when targets *do* wish to invoke a legal process), proactive initiatives aimed at structural issues will also be essential. These include: (i) appropriate regulation of internet service

providers (ISPs) to mandate greater transparency and accountability, and to minimize intrusions on privacy that complicate women's and girls' ability to control access to and use of information about themselves; and (ii) educational initiatives and expanded opportunities for informed public dialogue to address the underlying causes that disproportionately expose women and girls to violence, such as sexism, racism, homophobia, colonialism, and all of their intersections.

II. CANADIAN LEGISLATIVE MODELS AND CRIMINAL LAW JURISPRUDENCE

- 7) Canada invested early in what was then referred to as the “information super highway”, and considered technology an essential economic tool for creating future growth. As such, it was one of the first countries in the world to connect its schools to the internet and to provide a wide range of community access points (Bailey, 2016 at 3-4). By the late 1990s, however, the negative consequences of connectivity, including online hate speech, luring, child pornography, made their way into Canadian policymaking and debate. “Cyberbullying” has more recently made its way into public consciousness and debate as the result of a number of high profile suicides, some of which were associated with TFVAWG (Bailey, 2016 at 5; Bailey, 2015). In some cases, the connection between existing structures of discrimination and TFVAWG has been recognized and led to calls for both reactive legal responses to individual cases *and* a more broadly-based proactive strategy for addressing underlying causes (Bailey, 2015). Below we provide an overview of legal and policy responses to “cyberviolence” and “cyberbullying”, most of which are not specific to TFVAWG, but are nevertheless applicable to many of its forms.
- 8) ***Human rights law*** – TFVAWG can take the form of online hate propagation in which women or girls are targeted on the basis of gender and/or their membership or perceived membership in groups identifiable on the basis of social locations such as race, ethnicity, sexual orientation, gender identity, and so forth. Unfortunately, in 2013 Canada repealed s. 13 of the *Canadian Human Rights Act*, which provided a remedy for internet attacks of these kind (Bailey, 2016).⁴ In so doing, they removed the kind of proactive, human rights based approach to identity-based online attacks that many researchers and advocates had been calling for in light of growing concern around TFVAWG and cyberviolence more generally (Bailey, 2016). While provincial and territorial human rights codes forbid discriminatory displays, broadcasts or publications, it is not clear that all of these provisions would apply to internet-based attacks because internet communication falls within federal jurisdiction (Bailey, 2016). However, institutions, such as schools, that are

⁴ On November 18, 2016, the Committee on Elimination of Discrimination against Women recommended that Canada “review and amend legislation in order to provide adequate remedies to victims of cyber violence and reintroduce section 13 of the Canadian Human Rights Act” (CEDAW, 2016).

obligated to provide harassment-free environments can also face human rights tribunal orders relating to TFVAWG that is grounded in discrimination on prohibited grounds, such as gender (Bailey, 2016 at 12).

- 9) **Education law** – One proactive way of addressing TFVAWG is to incorporate education about it and its underlying causes into school curriculum. Education legislation in all provinces and territories (save one)⁵ specifically refers to “bullying” and “cyberbullying” and/or requires that schools and/or school boards address these issues. Further, all provincial and territorial ministries of education have “committed themselves to promoting respect for equity and diversity through safe, caring and accepting schools policies or through the articulation of principles requiring respect for difference” (Bailey, 2016 at 13-14). However, exactly how these commitments are manifesting in practice and whether they are encouraging greater or lesser reliance on surveillance mechanisms that disproportionately negatively expose students from vulnerable communities to monitoring and punishment remains of concern (Bailey, 2017). Further, none appear to focus on explicitly discussing discriminatory structures that compromise women’s and girls’ equal participation in an increasingly digitally connected world.

- 10) **Civil legal recourse** – Targets of certain forms of TFVAWG may be able to initiate civil litigation in court against their attackers in order to recover money for injuries sustained due to being attacked, although the costs, publicity and delay associated with legal action make it an unattractive, if not unattainable, remedy for most (Bailey, 2016 at 33). Where women or girls who are in a position to sue are unable to identify their attacker in order to initiate an action, they may bring a motion for a Norwich order to compel the attacker’s service provider to disclose identifying information associated with the account from which the attack was launched.⁶ Notable Canadian examples falling under this avenue include recourse relating to:
 - a) *privacy and intimate images* – Certain forms of TFVAWG, such as non-consensual distribution of intimate images, compromise the target’s dignity and privacy, sometimes exposing them to further harassment, violence and conflict with others in their lives (Bailey, 2016). British Columbia, Manitoba, Newfoundland and Saskatchewan’s privacy legislation creates a right to sue for invasion of privacy. Further, Manitoba’s *Intimate Image Protection Act* makes it a tort to non-consensually distribute another’s intimate image.

⁵ Nunavut’s *Education Act* does not specifically address “bullying” or “cyberbullying”. However, “these behaviours clearly fall within broader Indigenous laws, principles, and expectations set out in policies and statements relating to students’ rights and responsibilities” in Nunavut: Bailey, 2016 at 13.

⁶ The criteria for obtaining a Norwich order is set out in *GEA Group AG v Flex-N-Gate Corporation*, 2009 ONCA 619 at para 51; *York University v Bell Canada Enterprises*, 99 OR (3d) 695 (SC) at para.13.

- (Bailey 2016 at 34). In Ontario, a court found that a woman targeted by non-consensual disclosure of intimate images could sue her ex-partner for breach of confidence, intentional infliction of mental distress, and public disclosure of private facts in a case that will now be retried (Bailey, 2016 at 35). Finally, the Supreme Court of Canada in *AB v Bragg Communications Inc.* addressed one of the key drawbacks for young people considering suing for non-consensual distribution – the risk of further publicity – by finding that a 15-year-old girl targeted by a fake Facebook page could proceed under a pseudonym. In so doing, it recognized that “young victims of sexualized bullying are particularly vulnerable when their names are republished” (Bailey, 2016 at 36);
- b) *defamation* – Targets of TFVAWG who suffer reputational harm from online communication of false statements about them may be able to recover damages in a civil action for defamation (Bailey, 2016 at 36);
 - c) *copyright violation* – Where TFVAWG incorporates distribution of the target’s original works (e.g. a photograph taken by the target of herself) without the target’s consent the *Copyright Act* may entitle the target to an injunction and to damages (Bailey, 2016 at 37);
 - d) *tort of “cyberbullying”* – In 2013, Nova Scotia passed the *Cyber-safety Act*, which aimed to address “cyberbullying”, which was broadly defined under the legislation to include “any electronic communication ... that is intended or ought reasonably to have been expected to cause fear, intimidation, humiliation, distress or other damage to another person’s health, emotional well-being, self-esteem or reputation” (Bailey, 2016 at 37). However, the *Act* was struck down as unconstitutional on the basis that it was too broad and therefore violated life, liberty and security of the person and unduly restricted freedom of expression that are guaranteed by Canada’s *Charter of Rights and Freedoms* (Bailey, 2016 at 38); and
 - e) *negligence* – Schools or other institutions that fail to take due care to prevent physical or emotional harm to students or others to whom they owe responsibilities could be found liable for TFVAWG committed against those persons (Bailey, 2016 at 38-9).
- 11) ***Regulatory & administrative remedies*** – Provincial and federal privacy commissioners may also become involved in TFVAWG cases that involve alleged failures by private and public sector organizations to comply with rules around the collection, use and disclosure of personal information (Bailey, 2016 at 40). Both Manitoba and Nova Scotia have regulatory bodies specifically created to assist targets of non-consensual distribution of intimate images in getting those images removed or deleted (Bailey, 2016 at 40). However, since Nova Scotia’s *Cyber-safety Act* was struck down as unconstitutional, its regulatory body focuses more on education, public awareness and re-directing inquiries to other agencies (such as law

enforcement) for assistance (Bailey, 2016 at 41).

- 12) ***Criminal law responses*** – While no single provision in Canada’s *Criminal Code* addresses TFVAWG in all of its forms, many forms of TFVAWG include behaviours that are criminally prohibited in Canada. Too often, however, police do little to respond to reports of TFVAWG, notwithstanding the existence of criminal law provisions that apply (Keats Citron, 2014; McKenna, 2017). As a result, the published jurisprudence represents only a fraction of TFVAWG reported to authorities, and an even smaller fraction of all TFVAWG that is actually committed.
- 13) Our 2017 review of reported Canadian criminal law decisions yielded 114 cases involving TFVAWG. These involved charges of criminal harassment, extortion, voyeurism, sexual assault, non-consensual distribution of intimate images, defamatory libel, identity fraud, human trafficking, advertising sexual services, mischief in relation to data, and a set of 51 cases involving offences against minors, including sexual interference, invitation to sexual touching, sexual exploitation, child luring and child pornography (Bailey and Mathen, 2017 at 3-4). In 42 cases the victim was specifically identified as a girl, while in 48 cases the victim was specifically identified as a woman.⁷ In 106 of these cases the accused were male, while in 7 cases the accused were female and in 1 case a man and a woman were co-accused (Bailey and Mathen, 2017 at 4). Given the under-reporting of sexual violence, as well as the fact that many criminal law decisions are not made available online, this body of cases almost certainly represents only a fraction of instances of TFVAWG in Canada. Nonetheless, several themes were notable in the group of cases identified:
 - a) the use of technology by perpetrators that ranged from small devices used to surreptitiously record images to online posting of materials that exposed the material to potentially millions of people;
 - b) capture or control of the target’s personal information, including images non-consensually shared, but also manipulation of her information by lying, stealing or sometimes disseminating it;
 - c) undermining the agency and autonomy of the target by, for example, taking or distributing images of her without her consent or using her information without consultation;
 - d) objectification of the target as a “sexual object” or the taking of something intimate, valuable and personal to the target and using that against her, frequently in a way that robbed her of her autonomy and sexual integrity, often occasioning psychological harm that interfered with her health or well-

⁷ Some of the reported judgments involving multiple victims did not specify the ages of the victims.

- being in order for the accused to use the thing taken to his own ends;
- e) a gender component that went beyond the fact that the accused were overwhelmingly male and the targets overwhelmingly female, culminating in reproduction of “patterns of oppressing, silencing and demeaning women that are endemic in a patriarchal culture” (Bailey and Mathen, 2017 at 20-21); and
 - f) an emerging recognition in some cases that the “near-limitless reach of the internet multiplies, exponentially, the harm to one’s reputation, social standing, future prospects, personal relationships and, even, personal security when intimate information (or in some cases, misinformation) about her is distributed through those means. The sheer magnitude of the exposure can itself be understood as an aggravating factor – transforming what might ordinarily be understood as a private law harm (say, defamation) to a criminal law one” (Bailey and Mathen, 2017 at 22).
- 14) Several shortcomings in criminal law responses were also noted in the related jurisprudence, some of which are familiar from criminal cases involving VAW more generally:
- a) the need in voyeurism cases to prove the photos were taken for a “sexual purpose”, where photos are taken in situations where nudity or sexual activity would not ordinarily be expected to take place, and the failure of some courts to recognize that disproportionate targeting of women’s and girls’ breasts and other body parts is sufficient to establish such a purpose (Bailey and Mathen, 2017 at 5);
 - b) the failure of some courts, in assessing whether a target reasonably feared for her safety in criminal harassment cases, to take into account the seamless integration of online/offline activities that make it quite reasonable for a woman whose online activities are being closely monitored or who is receiving repeated communications to reasonably fear for her safety even if the accused is not known to be physically near or present (Bailey and Mathen, 2017 at 28);
 - c) suggestions in some cases that targets brought harassment on themselves or waived their privacy rights by participating online in the first place (Bailey and Mathen, 2017 at 29-30);
 - d) a tendency in some cases to minimize the violence at play in a particular case because it involved psychological harms that the court considered less serious than physical bodily ones (Bailey and Mathen, 2017 at 34-35); and
 - e) an innocence narrative present in a number of cases that prioritized harms to girls as public harms while minimizing harms to women as individualized harms, sometimes resulting in shifting responsibility onto the target for the

harms that she suffered, simply by virtue of her participation online (Bailey and Mathen, 2017 at 39-40).

- 15) Finally, it is noteworthy in the Canadian context that amendment of the *Criminal Code* to prohibit non-consensual distribution of intimate images came at the cost of significant expansion of law enforcement powers. While the negative consequences of TFVAWG (labeled “cyberbullying” by the then-federal government) were used to gain support for passage of the legislation, the amendments also expanded state monitoring and surveillance powers in general, rather than reserving use of those powers to cases involving TFVAWG (Throop, 2014).

III. INTERNET SERVICE PROVIDER POLICIES AND BUSINESS MODELS

- 16) ***Service provider responses*** - Women and girls can report online violence and sexual harassment to the social media platforms where the violence or harassment occurred because most social media platforms have a “report” option for violent or sexual content that users find harmful (Horsman, 2017).⁸ Two recent examples of service provider initiatives to address TFVAWG relate to:
 - a) *preventing fraudulent impersonation* - Twitter’s “blue verified” badge identifies a user’s account as *the* authentic account under that name, making impersonation accounts easy to identify (Twitter, 2017). However, this verification system is limited to “accounts of public interest” so while well-known women and girls may benefit, the average user would not have access to verification (Dunn, Lalonde and Bailey, 2017 at 89); and
 - b) *non-consensual distribution of intimate images* - Facebook has developed a specific reporting tool for intimate images shared without consent. If an image is deemed to violate Facebook’s Community Standards, then “in most cases” the company will disable the account that posted the image and use photo-matching technology to remove not only the image originally reported, but any copies of the image posted across the company’s platforms including Facebook, Messenger and Instagram (Davis, 2017).
- 17) ***Problems with service provider responses*** – reliance on service providers to address TFVAWG and the processes for making those reports raises a variety of concerns:
 - a) *private processes supplanting public law and policy* - police deference to the decisions service providers make and the standards that they set in their terms of service could undermine the rights of women and girls under Canadian law. It is unclear how often this is happening. However, in one case

⁸ For examples of reporting options for women and girls see: OCTEVAW. 2017. “Tech Without Violence.” Accessed September 26, 2017. <http://www.techwithoutviolence.ca/>.

when a woman reported to police that she was being harassed and impersonated on Twitter, they referred her to Twitter's policy on how to report harassment. The police further indicated that if Twitter allowed parody accounts (suggesting the accounts she was filing a complaint about were a parody), there was "nothing they could do about [her] impersonators", despite there being clear laws against the behavior. When she pressed for further action, the police invited her to file a report for "statistical purposes" (Dunn, Lalonde and Bailey, 2017 at 89);

- b) *lack of accountability* - platform reporting processes are generally non-transparent, making it difficult for women and girls to understand which actions against them will be considered a violation (Athar 2015 at 20). The internal guidelines used by companies such as Facebook are not made public by the company and the "Community Standards" policies that are publicly available are usually vague and opaque.⁹ As a result, it is nearly impossible to be sure which content will be considered a violation, which also raises important questions as to the bases upon which expression is being restricted. Where machine-based decision-making is used, the reasoning behind these decisions is even more inaccessible (O'Neil, 2016);
- c) *ineffectiveness* - women and girls report that platforms rarely take action against the violence or harassment they experience once it has been reported (Hess, 2014); and
- d) *questionable standards and insufficient staffing* - even moderators hired by social media companies with access to the company policies face difficulties interpreting which content violates those policies and which does not. For example, in May 2017, The Guardian newspaper obtained and released portions of internal manuals of Facebook's reporting procedures. The manuals showed that Facebook had created a system to determine which violent statements could "cause real world harm" and should be removed. However, these documents demonstrated that even explicitly violent content such as "To snap a bitch's neck, make sure you apply all your pressure to the middle of her throat" was not considered "credible" violent commentary that should be removed (The Guardian, 2017). Some staff monitoring these reports found the guidelines unclear, particularly those around sexual content, and felt unprepared to manage the level of reports and the graphic content of the reported violations (Hopkins, 2017). The limited number of staff monitoring violations in contrast to the voluminous amounts of reports further problematizes this leading to mistakes by staff (Hopkins, 2017; Grierson, 2017).

IV. PROACTIVE APPROACHES TARGETING DISCRIMINATORY STRUCTURES

⁹ For example, see the vague language of Facebook: Facebook. "Community Standards." 2018. Accessed September 26, 2017. <https://www.facebook.com/communitystandards>.

- 18) Recognizing that violence against women and girls can be facilitated not just physically, but technologically is an essential first step toward addressing this form of invasion on women's privacy, equality, sexual integrity and autonomy. Law can play an important role in articulating local, national and international concern about these fundamental issues as can responsibly regulated and publicly accountable industry players. That said, moving beyond reactive responses to TFVAWG by taking proactive steps to address underlying discriminatory root causes will also be essential. Here we highlight three examples of the kinds of collaborative responses that hold promise for contributing to the social transformation that will be necessary to end gender-based violence.
- 19) In 2014, Status of Women Canada announced funding for projects aimed at ending cyberviolence against women and girls (Status of Women Canada, 2014-2015). Among the recipients of those grants were YWCA Canada and OCTEVAW, both of which produced needs assessment reports grounded in the lived experiences of girls and young women (Estable and Meyer, 2015; Fairbairn and Black, 2015). Each then went on to produce unique and creative outcomes focused on creating proactive change:
- a) in 2016, the YWCA launched a series of resources relating to TFVAWG, aimed at generating dialogue and debate, recognition and accreditation of girls' and young women's knowledge, creating a culture of empathy across industry and disseminating knowledge about rights to girls, young women and the adults who support them. These included a [Rights Guide for Girls, Young Women and Gender Nonconforming Youth](#),¹⁰ a video entitled [#PressPaws on Cyberviolence](#)¹¹ co-created with grassroots collectives Project Slut and femifesto, and a [Guide for Trusted Adults](#)¹² on practical tips for supporting girls and young women navigating online life, co-created with Canada's leading digital literacy educator, MediaSmarts;
 - b) in 2016, OCTEVAW launched its [Tech Without Violence Prevention Framework](#),¹³ co-created with the Ottawa Youth Service Bureau's Purple Sisters (an organization of young women and other gender variant youth). The Framework, which is accessible online, sets out four pillars for preventing cyberviolence, including: prevention, response, privacy and support. Grounded in the experiences of young women and members of the LGBTQ youth, the Framework stresses what the information and

¹⁰ The Rights Guide can be found online here: < <http://ywcarightsguide.ca>>.

¹¹ The #PressPaws video can be found online here: < <https://www.youtube.com/watch?v=0NzXHk2rzuE>>.

¹² The Guide for Trusted Adults can be found online here: < <http://ywcaCanada.ca/data/documents/00000543.pdf>>.

¹³ The website relating to the Tech Without Violence Framework can be found online here: < <http://www.techwithoutviolence.ca/tech-without-violence-prevention-framework>>.

communications technology sector can do to help prevent and eliminate gender-based violence and harassment. These include developing transparent and effective reporting mechanisms and community standards, and fair terms of service (OCTEVAW, 2016). The website also incorporates a variety of resources, including guides on social media, dating apps, and online safety tips; and

- 20) in 2015, MediaSmarts, in collaboration with The eGirls Project, created the "[Half Girl, Half Face Workshop](#)"¹⁴ intended for girls in grades 7 to 9. Freely available online, it provides educators with a video and facilitator's guide to support peer-led discussions and activities revolving around the story of a teen whose image has gone viral on social media. The workshop creates opportunities for opening up dialogue and discussion around privacy, publicity, inclusion and exclusion as girls and young women navigate the complex terrain of online social media.

V. CONCLUSION AND RECOMMENDATIONS

- 21) TFVAWG must be recognized as *violence* and *discrimination* within the meaning of international instruments aimed at ensuring women's and girls' full and equal enjoyment of all human rights and freedoms. The consequences of TFVAWG involve both individual physical, psychological and sexual harms, and occasion societal harm by attacking women's and girls' autonomy, privacy and free expression in ways that undermine their ability to contribute equally to private and public life.
- 22) An ecosystem of law, social norms, markets and architectures individually and in combination affects behaviours and outcomes in our increasingly digitally networked world (Lessig, 2006). So too does this ecosystem affect TFVAWG. While individual perpetrators can and should be held to account, meaningfully addressing TFVAWG at local, national and international levels will require not only reactive responses to individuals, but industry regulation to improve accountability and transparency, as well as proactive measures to address underlying discriminatory social structures and practices.
- 23) We recommend development of a multi-pronged policy approach to TFVAWG that recognizes that while *legal* responses can serve to publicly communicate women's and girls' place and value in the community, law alone will not meaningfully respond to the needs and aspirations of *all* women and girls. Instead, law should form part of a more comprehensive strategy that:

¹⁴ The Half Girl, Half Face Workshop materials can be found online here: <
<http://mediasmarts.ca/digital-media-literacy/e-tutorials/half-girl-half-face-workshop>>.

- a) directly engages girls and women from a wide spectrum of social locations and ages in the policy-making process¹⁵ in order to ensure that the impacts of interlocking axes of discrimination that inform the lived reality of girls and women are meaningfully integrated;
- b) moves toward approaches focused on the responsibility of the community and individual perpetrators for TFVAWG, rather than shifting it onto girls and women themselves;
- c) improves the responsiveness of criminal legal recourse by:
 - i) ensuring that law enforcement officers are properly trained and resourced in receiving and evaluating TFVAWG reports, and are clear that industry terms of service do not in any case override criminal law; and
 - ii) ensuring that judges are familiarized with the social context relevant to TFVAWG, including the seamless integration of “online/offline” in girls’ and women’s lives and the right of girls and women to participate in our digitally networked society free of violence and discrimination;
- d) ensures that TFVAWG does not become an excuse for unnecessary expansion of police powers and surveillance;
- e) recognizes the importance of the proactive role that law can play in the ecosystem that incubates TFVAWG by:
 - i) developing (or in Canada’s case, reinstating) human rights based complaints mechanisms and educational responses to address discriminatory behaviours and structures that underlie TFVAWG; and
 - ii) implementing education law and curriculum focused explicitly on women’s and girls’ equal rights to public participation, privacy, free expression and autonomy, and the discriminatory behaviours and structures that underlie TFVAWG;
- f) recognizes and addresses the role that the “data in exchange for services” commercial model that currently characterizes digital networks plays in shaping the environment in ways that can expose girls and women to TFVAWG. Regulation of online service providers should be improved to mandate greater transparency and accountability in their collection, use and distribution of users’ data, and in their responses to TFVAWG complaints. These measures will become increasingly urgent as service providers continue to move toward machine-based algorithmic decision-making, which will compromise their ability to provide explanations for their decisions in

¹⁵ Under Article 3 of the UN Convention on the Rights of the Child children have the right to participate in processes that affect them and to have their best interests protected. Further, the UN Committee on the Rights of the Child requires signatory states to “pay special attention to the girl child to be heard, to receive support, if needed, to voice her view and her view be given due weight”: UN Committee on the Rights of the Child, 2009 at para 77.

terms understandable to humans; and

- g) recognizes and values grassroots community knowledge and collaboration as essential to the development of responses to TFVAWG that are meaningful to girls and women from a wide spectrum of social locations by:
- i) actively engaging community organizations in policy-making processes and ensuring them adequate resources to participate on a equal footing with industry in these processes; and
 - ii) providing funding and other resources to these organizations to support their research, and individual and collaborative initiatives.

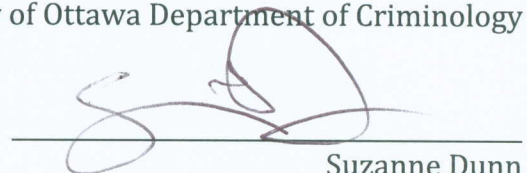
All of which is respectfully submitted,



Jane Bailey
Professor, University of Ottawa Faculty of Law



Valerie Steeves
Professor, University of Ottawa Department of Criminology



Suzanne Dunn
PhD Student, University of Ottawa Faculty of Law

References

- Asia Eaton, Holly Jacobs and Yanet Ruvalcaba. 2017. *2017 Nationwide Online Study of Nonconsensual Porn Victimization and Perpetration*. (Cyber Civil Rights Initiative: 2017). <https://www.cybercivilrights.org/wp-content/uploads/2017/06/CCRI-2017-Research-Report.pdf>.
- Athar, Rima. 2015. "End Violence: Women's Rights and Safety Online- From Impunity to Justice: Improving Corporate Policies to End Technology-Related Violence Against Women." *Association for Progressive Communications*.
- Bailey, Jane and Valerie Steeves. 2015. *eGirls, eCitizens*. Ottawa: University of Ottawa Press.
- Bailey, Jane. 2014. "Time to Unpack the Juggernaut? Reflections on the Canadian Federal Parliamentary Debates on 'Cyberbullying.'" *The Dalhousie Law Journal* 37: 661–707.
- Bailey, Jane. 2015. "A Perfect Storm: How the Online Environment, Social Norms, and Law Shape Girls' Lives." In *eGirls, eCitizens*, edited by Jane Bailey, and Valerie Steeves, 21–54. Ottawa: University of Ottawa Press.
- Bailey, Jane. 2016. "Canadian Legal Approaches to 'Cyberbullying' and Cyberviolence: An Overview." *Ottawa Faculty of Law Working Paper* No. 2016–37. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2841413.
- Bailey, Jane. 2016. Submissions to the House of Commons Standing Committee on the Status of Women Relating to Violence Against Young Women and Girls in Canada. June 16, 2016. <http://www.equalityproject.ca/wp-content/uploads/2016/06/Submissions-of-Jane-Bailey.pdf>.
- Bailey, Jane. 2017. "From 'zero tolerance' to 'safe and accepting': Surveillance and equity implications of educational policy related to 'cyberbullying'." *Education Law Journal* 26: 147-180.
- Bailey, Jane and Carissima Mathen. 2017. "Technologically-facilitated Violence Against Women & Girls: If Criminal Law Can Respond, Should It?" [unpublished, copy on file with the authors].
- Canadian Women's Foundation. 2014. *The Facts About Violence Against Women*. <http://www.canadianwomen.org/facts-about-violence>.
- Committee on the Elimination of Discrimination against Women (CEDAW), *Concluding observations on the combined eighth and ninth periodic reports of Canada*, 18 November 2016, CEDAW/C/CAN/CO/8-9.

Cyber Civil Rights Initiative. 2014. *End Revenge Porn*.
<https://www.cybercivilrights.org/wp-content/uploads/2014/12/RPStatistics.pdf>.

Davis, Antigone. 2017. "Using technology to protect intimate images and help build a safe community." *Facebook Newsroom*. April 5, 2017.
<https://newsroom.fb.com/news/2017/04/using-technology-to-protect-intimate-images-and-help-build-a-safe-community/>.

Dunn, Suzanne, Julie Lalonde and Jane Bailey. 2017. "Terms of Silence: Weaknesses in Corporate and Law Enforcement Responses to Cyberviolence against Girls." *Girlhood Studies* 10, no. 2: 80-96.

Estable, Alma, and Mechthild Meyer. 2015. *Creating a Safer Digital World for Young Women*. YWCA Canada. <http://ywcacanada.ca/data/documents/00000460.pdf>.

Facebook. "Community Standards." 2018. Accessed September 26, 2017.
<https://www.facebook.com/communitystandards>.

Fairbairn, Jordan, and Dillon Black. 2015. *Cyberviolence against Women & Girls*. Ottawa Coalition to End Violence against Women. http://www.octevaw-cocvff.ca/sites/default/files/CyberViolenceReport_OCTEVAW.pdf.

GEA Group AG v Flex-N-Gate Corporation, 2009 ONCA 619.

Government of Canada. 2016. *Study: Cyberbullying and cyberstalking among Internet users aged 15 to 29 in Canada*. Statistics Canada. <http://www.statcan.gc.ca/daily-quotidien/161219/dq161219a-eng.htm>.

Grierson, Jamie. 2017. "'No grey areas': experts urge Facebook to change moderation policies." *The Guardian*. May 22, 2017.
<https://www.theguardian.com/news/2017/may/22/no-grey-areas-experts-urge-facebook-to-change-moderation-policies>.

Hess, Amanda. "Why women aren't welcome on the internet." 2014. *Pacific Standard*. January 6, 2014. <https://psmag.com/why-women-aren-t-welcome-on-theinternet-aa21fdbc8d6>.

Hopkins, Nick. 2017. "Facebook moderators: a quick guide to their job and its challenges." *The Guardian*. May 21, 2017.
<https://www.theguardian.com/news/2017/may/21/facebook-moderators-quick-guide-job-challenges>.

Horsman, Graeme. 2017. "A survey of current social network and online communication provision policies to support law enforcement identify offenders." *Digital Investigation* 21: 65-75.

Keats Citron, Danielle. 2014. *Hate Crimes in Cyberspace*. Boston: Harvard University Press.

Lessig, Lawrence. 2006. *Code: Version 2.0*. New York: Basic Books.

Mazowita, Benjamin and Mireille Vézina. 2012. *Police-reported cybercrime in Canada*. Statistics Canada. <http://www.statcan.gc.ca/pub/85-002-x/2014001/article/14093-eng.pdf>.

McKenna, Kate. 2017. "Montreal woman terrified her personal info was posted in escort ads. Did police do enough?" *CBC News*. September 7, 2017. <http://www.cbc.ca/news/canada/montreal/montreal-woman-terrified-her-personal-info-was-posted-in-escort-ads-did-police-do-enough-1.4276602>.

MediaSmarts. 2015. *Half Girl, Half Face Workshop*. <http://mediasmarts.ca/digital-media-literacy/e-tutorials/half-girl-half-face-workshop>.

O'Neil, Cathy. 2016. *Weapons of Math Destruction: How Big Data Increase Inequality and Threatens Democracy*. New York: Crown.

OCTEVAW. 2017. "Tech Without Violence." <http://www.techwithoutviolence.ca/>.

OCTEVAW and Ottawa Youth Service Bureau's Purple Sisters. 2016. *Tech Without Violence Prevention Framework*. <http://www.techwithoutviolence.ca/tech-without-violence-prevention-framework>.

Powell, Anastasia and Nicola Henry. 2015. *Digital harassment and abuse of adult Australians: A summary report*. RMIT University.

Status of Women Canada 2014-2015. *Funded Projects*. <http://www.swc-cfc.gc.ca/fun-fin/projects-projets/index-en.html>.

Steeves, Valerie. 2014. *Young Canadians in a Wired World, Phase III: Cyberbullying: Dealing with Online Meanness, Cruelty and Threats*. MediaSmarts. http://mediasmarts.ca/sites/mediasmarts/files/pdfs/publication-report/full/YCWWIII_Cyberbullying_FullReport.pdf.

The Guardian. 2017. "Facebook's manual on credible threats of violence." *The Guardian*. May 21, 2017. <https://www.theguardian.com/news/gallery/2017/may/21/facebooks-manual-on-credible-threats-of-violence>.

Throop, Brett. 2014. "Cyberbullying has 'hugely disproportionate impact on women and girls.'" *CIBC News*. August 8, 2014. <http://www.cbc.ca/news/cyberbullying-has-hugely-disproportionate-impact-on-women-and-girls-1.2731195>.

Twitter. 2017. "About verified accounts." Accessed September 26, 2017.
<https://support.twitter.com/groups/31-twitter-basics/topics/111-features/articles/119135-about-verified-accounts>.

UNICEF. 1999. *Oslo Challenge*. <https://www.unicef.org/magic/briefing/oslo.html>.

United Nations Committee on the Rights of the Child, *Convention on the Rights of the Child*, GA Res 40/25, UN GAOR, 44th Sess., U.N. Doc A/RES/44/25 (New York: United Nations Office of the High Commissioner for Human Rights, 1990).
<http://www.ohchr.org/en/professionalinterest/pages/crc.aspx>.

United Nations Committee on the Rights of the Child, *The Right of the Child to be Heard*, CRC, 55 Sess., General Comment No 12 UN Doc CRC/C/GC/12 (New York: United Nations Convention on the Rights of the Child, 2009).
<http://www2.ohchr.org/english/bodies/crc/docs/AdvanceVersions/CRC-C-GC-12.pdf>.

United Nations General Assembly, *Convention on the Elimination of All Forms of Discrimination Against Women*, 18 December 1979, United Nations, Treaty Series, vol. 1249. <http://www.refworld.org/docid/3ae6b3970>.

United Nations General Assembly, *Declaration on the Elimination of Violence against Women*, 20 December 1993, A/RES/48/104.
<http://www.refworld.org/docid/3b00f25d2c.html>.

West, Jessica. 2014. *Cyber-Violence Against Women*. Battered Women's Support Services. <http://www.bwss.org/wp-content/uploads/2014/05/CyberVAWReportJessicaWest.pdf>.

York University v Bell Canada Enterprises, 99 OR (3d) 695 (SC).

YWCA Canada and MediaSmarts. 2017. *Guide for Trusted Adults*.
<http://mediasmarts.ca/sites/mediasmarts/files/guides/ywca-guide-for-trusted-adults.pdf>.

YWCA Canada, Project Slut, femifesto. 2016. "#PressPaws on Cyberviolence".
<https://www.youtube.com/watch?v=0NzXHk2rzuE>.

YWCA. 2016. Canada. *Rights Guide for Girls, Young Women and Gender Nonconforming Youth*. <http://ywcarightsguide.ca>.