Cyberviolence against women and girls is linked to the larger social issue of violence against women and girls. Cyberspaces, such as social media sites, do not cause cyber violence, but impact the ways in which it occurs.

Ottawa Coalition to End Violence Against Women

May 2015
OCTEVAW is a coalition of organizations and individuals working together to help strengthen a coordinated response to violence against women and girls in the city. The Coalition’s membership connects regularly to ensure that there are strong channels of communication for information sharing among different organizations and sectors in the city, including front-line organizations such as the shelters and community centres that provide critical care and support, as well as institutions including the Ottawa Hospital and the Ottawa Police Service who provide a critical response to the issue from a criminal justice and physical health perspective.

Report Authors:
Jordan Fairbairn, PhD Candidate, Carleton University for Secondary Data Review & Dillon Black, OCTEVAW for Youth Engagement Process & Working with Young Women in Ottawa

The authors would like to gratefully acknowledge the support and confidence of Status of Women Canada in selecting the Ottawa Coalition to End Violence Against Women (OCTEVAW) for the Preventing Cyberviolence Against Women & Girls Project. It is our sincere hope that this project will continue to contribute to our understanding and continued development and implementation of strategies to prevent violence against young women & girls in Ottawa.

The ideas and opinions expressed in this work are those of the authors and do not necessarily reflect the views of the Government of Canada. We are grateful to Ottawa communities, young people, students, interviewees, key informants and participants who gave generously of their time and expertise to the Needs Assessment process. It could not have been conducted without their involvement and ongoing commitment to ending violence against women & girls.
Meet the Youth Advisory Committee!

Join the Purple Sisters on Facebook
and on Twitter!

The Purple Sisters Youth Advisory works to increase awareness of young women's issues in the community. Issues such as abuse, inequalities in the workplace, legal systems and schools systems are not new, but they are still significant. While progress has been made, we must continue the fight against abuse and inequality with commitment and passion.

The Purple Sisters bring attention to these issues in an environment that may otherwise allow them to become overshadowed by more recent and publicized issues affecting women — for instance, those related to sexuality or race. This group partners with young women and the organizations that serve them to offer education sessions, workshops, events and activities that promote an understanding of current women's issues.
Cyberviolence Against Women & Girls Project

Acknowledgment.................................................................................................................. Error! Bookmark not defined.

Project Partners ...................................................................................................................... 5

About this Project .................................................................................................................... 6

Doing Youth Engagement ....................................................................................................... 7

Report Findings ..................................................................................................................... 11

Background ............................................................................................................................. 16

Overview of Social Media ....................................................................................................... 10

Young Canadians in a Wired World ....................................................................................... 11

Part 1: Cyberviolence: What it is and what do we know? ....................................................... 14

Online sexual harassment ....................................................................................................... 15

Non-consensual sharing of intimate images (often called revenge porn) ............................... 16

Recording and distribution of sexual assault .......................................................................... 17

Cyberstalking and digital dating abuse ................................................................................... 18

Summary: ................................................................................................................................. 21

Part 2: Emerging Issues Highlighted by Media Coverage of Cyberviolence ............................ 21

Harassment of sexual assault survivors .................................................................................. 22

Hookup culture, sexuality, and online dating .......................................................................... 24

Anonymity and online harassment ......................................................................................... 25

Gendered and sexualized violence as entertainment ............................................................... 27

Part 3: Responses to Cyberviolence ....................................................................................... 29

Government responses .......................................................................................................... 29

Legal responses ....................................................................................................................... 30

Community responses .......................................................................................................... 31

Individual strategies .............................................................................................................. 32

Technological responses ....................................................................................................... 33

Research findings and recommendations .............................................................................. 34

Part 4: Let’s Tech About It: Social Media Governance ............................................................ 36

Impact of social media structures .......................................................................................... 36

Social media policies to address cyberviolence ...................................................................... 38

Conclusion .............................................................................................................................. 47

Feasibility of a code of conduct model .................................................................................. 47

Emerging Themes .................................................................................................................... 56

Emerging Possibilities & Strategies ...................................................................................... 65

Bibliography ........................................................................................................................... 61

Appendix A: Take Back the Tech’s Ten Tips for Challenging Internet Based Gender

Discrimination and Online Harassment Against Women ...................................................... 69

Appendix B: TrollBusters ...................................................................................................... 71
PROJECT PARTNERS

Media Smarts

Jane Bailey & Valerie Steeves (egirls Project)

Carleton University Sexual Assault Support Centre

Sisters Achieving Excellence (SAE)

Rena Bivens, Carleton University

Youth Services Bureau

In Love & In Danger (Family Services Ottawa)

Jordan Fairbairn, Carleton University
ABOUT THIS PROJECT

This project is taking place in the city of Ottawa, where OCTEVAW has a network of organizations and individuals united by their commitment to respond to the needs of women and girls experiencing violence, and ultimately ending violence against women and girls. This project focuses on working towards improving the lives of young women and girls, in particular, by creating a strategy that can help transform digital spaces to be empowering and challenge and eliminate instances of cyberviolence.

In order to do this we are connecting with multiple communities in the city, including front-line service providers responding to the needs of women and girls experiencing violence, non-profit organizations who do programming with young women and girls, academics engaged in understanding the particular and gendered experiences of girls and young women with respect to cyberviolence, the technology business sector who help design, implement and govern platforms where cyberviolence may occur, and most importantly young women and girls themselves.

The need for this work to support young women and girls in Ottawa is critical. OCTEVAW in partnership with Crime Prevention Ottawa, recently released research by Jordan Fairbairn, Rena Bivens and Myrna Dawson entitled 'Sexual Violence and Social Media' which found that girls and young women 'appear to experience higher rates of sexual violence associated with social media' (p. 2), and that community-based organizations and front-line workers in the city, while aware of experiences of gender-based cyberviolence have not been tracking or monitoring its existence, specifically, and that more needs to be done to understand how diverse groups of young women and girls experience it based on other aspects of their identity such as mental health or social class (p. 3)


What is a Gender Based Analysis?

A Gender-Based Analysis (GBA) is an analytical tool that we have used within our process that structurally integrates a gender perspective into the development of policies, programs, services and legislation. It helps to assess differential impact and to identify the complex social barriers that women, men, and all genders experience. A gender-based analysis makes possible for policy, programming, and services to be undertaken with an appreciation of gender differences while promoting agency and self-determination.
DOING YOUTH ENGAGEMENT

The *Cyber and Sexual Violence: Helping Communities Respond* is organized in two primary phases to involve young people early on in shaping the project’s matters of concern, the first phase is our needs assessment and the second phase is the development and implementation of a strategy to address cyberviolence. The project goal is to understand the complex needs and experiences of young women and girls online, to identify whether digital media technologies and social media platforms have a responsibility to intervene in issues related to cyber and sexual violence, as well as the narratives produced and reproduced around issues of governance, digital media production, privacy, consent, and security as well as best practices to engage digital technology platforms in the prevention of cyberviolence.

Our approach was to involve young women and girls and centre their voices throughout this needs assessment process. To do so we chose to use a youth engagement model developed with the Youth Services Bureau of Ottawa as well as worked with the Purple Sisters Youth Advisory Committee (PSYAC) and engaged with other young women in Ottawa.

This model was guided by concerns such as what sort of relationships do young women and girls want to amplify and minimize in their own strategy development? What skills and knowledges are needed and how can they be cultivated? These were the some questions to be identified and deconstructed in our knowledge building workshops and continually engaged with throughout the needs assessment process and strategy development.

*The Purple Sisters Youth Advisory Committee*

The PSYAC ranged in age from 16 to 24, consisted mostly of young women and feminine identified people, immigrants or children of immigrants, and more than half of the group were people of colour and/or identified within the LGBTQ spectrum. Their motivations generally concerned wanting to know more about “how the Internet works,” and to learn something about their relationship with it as well as to figure out how to best engage with issues surrounding sexual violence in their communities, particularly online.

*Ethical Considerations for Youth Engagement*

The success of youth engagement efforts depends on whether youth engagement is practiced in an ethical, respectful way. If youth engagement efforts are merely tokenistic or superficial youth can end up feeling like they are not respected or involved. To ensure our project respectfully engages with young women, there are eight principles we follow based in youth engagement work to ensure our engagement process is practiced ethically:
**Guiding Intentions (developed with the Youth Services Bureau)**

*Youth Engagement is not a program*

Youth engagement should be viewed as a philosophy and natural way of working in the organization rather than as a special program.

*Contributions match the project goals*

Young people and adults who are working with us should be recruited for their knowledge, skills, interests and commitment to the organizational mission.

*One person cannot represent many*

A young person should not be considered “the youth voice” at the table- it should be acknowledged that everyone at the table brings different perspectives to the issue.

*Debate as a learning tool*

Debate is a key element of personal and organizational growth. Our youth engagement process is dedicated to learning and growing and being flexible and adaptable throughout this process.

*(Adapted from the Youth Services Bureau)*
BACKGROUND

Introduction

Sexual violence involving the Internet goes by many names: online sexual violence, online sexual harassment, gendered online violence, cyberviolence, cyber sexual violence, technology-related violence, sexualized cyberbullying, and so forth. In recent years, this violence has become widely recognized by service providers, activists, advocates, and researchers as a social problem requiring intervention. However, there are as of yet no systematized data collection practices in this area in Canada.

A review of the literature is intended to contribute to the needs assessment and strategy development for OCTEVAW’s Status of Women funded project “Cyber Violence Against Women and Girls” by exploring what research and news media coverage tell us about cyberviolence, what sorts of social responses have taken place to date, and the relationship between social media structures and policies and cyberviolence. For the purposes of consistency with the Status of Women project, this project will use the term cyberviolence, understanding that in this context the focus is on women and girls. Additionally, the focus here is consistent with the larger project focus on young women and girls between the ages of 16 and 24.

We know that the Internet and social media are important parts of society as a whole and that a majority of young people has grown up using the Internet. One study found that 90 percent of teenagers use the Internet regularly, and 70 percent have a user profile on at least one social networking site (Subrahmanyam et al., 2009). This meta-analysis also found that much violence involving youth (e.g. bullying, gang violence, harassment) increasingly occurs in online spaces (Subrahmanyam et al., 2009) and that much of this violence is gendered, racialized, or sexualized in nature (Fairbairn, Bivens, & Dawson, 2013).

Material for this inquiry was gathered through a combination of searches of the University of Toronto’s ProQuest database, Google Scholar, and Google News. A list of keywords and search terms used include combinations of the following terms: cyberviolence; online sexual violence; Canada; Ottawa; Facebook; Twitter; Tinder; sexual assault; social media; alcohol; safety; youth; teenagers; young people; sexual violence; prevention; confessional apps; sexual harassment; revenge porn. Given that online environments develop and change rapidly, it is important to consider current and emerging research on this area as much as possible. As such, this report focuses primarily on materials from within the past five years.

This report is divided into four substantive sections. The first section outlines cyberviolence in terms of what we know about this set of issues by breaking it down into three central components: online harassment, non-consensual distribution of intimate images, and cyberstalking/digital dating violence. The second section explores news coverage about cyber violence, highlighting specific themes of this coverage as well as social media sites and/or apps that are the focus of coverage. It also discusses several high profile media cases that have contributed to broader social awareness of cyberviolence against women and girls. The third section explores responses to cyberviolence across a variety of sectors. The fourth section summarizes emerging work on social media site governance: the ability of social media
structures and policies to address cyberviolence, and the extent and nature of social media companies’ responses to cyberviolence to date. First however, it briefly overviews social media and explores what we know about young people’s experiences online in Canada.

**Overview of social media**

The Internet in 2015 is extremely social, and has moved from a broadcast communication model to a user-generated content model where users are both producers and consumers of content. As such, this report focuses on social media. This literature uses the definition of social media from the report *Sexual Violence and Social Media: Building A Framework for Prevention* (Fairbairn, Bivens, and Dawson, 2013). Social media is a widely used term that can encompass many platforms. Here, it refers to “the wide range of Internet-based and mobile services that allow users to participate in online exchanges, contribute user-created content, or join online communities” (Dewing, 2012, p.1). Social media can be broken down into several categories of social media. This report focuses primarily on social network sites, media-sharing sites, and status-update services, as well as web-based applications (apps).

<table>
<thead>
<tr>
<th>Type of social media</th>
<th>Description</th>
<th>Popular examples in Canada</th>
</tr>
</thead>
<tbody>
<tr>
<td>Social network sites</td>
<td>Allow individuals to create a public or semi-public profile within a bounded system and connect with other users with whom they share a connection.</td>
<td>Facebook, LinkedIn</td>
</tr>
<tr>
<td>Media-sharing sites</td>
<td>Allow users to post videos or photographs that others can share, comment, or ‘like’.</td>
<td>YouTube, Instagram, Vine, Pinterest, Snapchat</td>
</tr>
<tr>
<td>Status-update services</td>
<td>Also known as microblogging services, allow users to share short updates (e.g. tweets) and to see updates of others.</td>
<td>Twitter</td>
</tr>
<tr>
<td>Messenger Apps</td>
<td>These are third party chat &amp; messenger apps used to communicate via SMS text messaging.</td>
<td>Facebook Messenger, Whisper, Burn Note, Kik, Yik Yak, What’s App</td>
</tr>
<tr>
<td>Blogs</td>
<td>An online journal often centered around core area(s) of interest where pages are usually displayed in reverse chronological order.</td>
<td>WordPress, Tumblr, Blogger</td>
</tr>
<tr>
<td>Social news</td>
<td>Forums where people post various news items or links to outside articles and users vote on the items. Items with the most votes are displayed most prominently.</td>
<td>reddit, Digg</td>
</tr>
<tr>
<td>Virtual world content</td>
<td>Offer game-like virtual environments in which users interact, often creating avatars (a virtual representation of the user) to interact with others.</td>
<td>Second Life</td>
</tr>
<tr>
<td>Wikis</td>
<td>A collective website where all participants are able to modify any page or create new pages.</td>
<td>Wikipedia</td>
</tr>
</tbody>
</table>

*Adapted from Dewing (2012)*
When we were speaking with young women they highlighted these apps as the most popular in their communities: Instagram, Twitter, Facebook, Tumblr, Kik, Yik Yak, Vine & Snapchat

Young Canadians in a Wired World

In 2013, MediaSmarts explored young people’s experiences and perceptions online by conducting a national survey Young Canadians in a Wired World with 5,436 Canadian students in grades 4 through 11 in every province and territory. Although this survey focuses on a generally younger demographic that that which OCTEVAW’s project is targeting (16-24), the findings are still worth highlighting as they represent the most extensive national survey of young people’s online experiences conducted in Canada to date.

What follows are selected findings from various reports published as part of the series Young Canadians in a Wired World (Steeves, 2014a, 2014b, 2014c, 2014d) and their relevance for informing OCTEVAW’s work.

Online Safety (Steeves, 2014c)

- Feelings of safety grow with age, from a low of 50 percent in grades 4 and 7 to a high of 66 percent in Grade 11.
- Girls are both more likely than boys to agree with the statement that they could be hurt by online strangers (82% compared to 63% of boys) and less likely to see the Internet as a safe place (51% compared to 61% of boys).
- Comparing grades, feelings of safety rise from a low of 50 percent in grades 4 and 7 to a high of 66 percent in Grade 11.
- Despite concerns about safety, high percentages of boys (90%) and girls (89%) agree with the statement “I know how to protect myself online”.

Best Practice: These findings suggest gender differences girls’ and boys’ perceptions of safety online, and that the older age range feels more safe. In general, students say they know how to protect themselves online. There is a need to better understand how sexual violence in particular relates to feelings of safety, and how individual safety strategies practiced by youth can be supported and enabled by social media sites design and governance (thus reducing the need for individual safety strategies).

Forwarding Sexts (Steeves, 2014a, 2014d)
(Data from grades 7-11 students only)

- Only four percent of students report that they have forwarded a sext that someone had sent them to someone else.
- Of the 24 percent of students in grades 7-11 with cell phones who have received a sext from its creator, only 15 percent forwarded it to someone else. That means that 85 percent of grade 7-11 students with cell phones who have received a sext created for them have not forwarded the sext to someone else.
• Although boys and girls are equally likely to create a sext, older students in general, and boys in particular, are more likely to receive them and to forward them to others.
• In the context of cyberbullying, MediaSmarts’ data suggests that the overlap between sexting and online meanness is quite small (Steeves, 2014a).
• Having a household rule about treating people online with respect does not correlate with a lower likelihood of forwarding sexts.

Best Practice: Forwarding sexts, without permission, is non-consensual distribution of intimate images (a form of cyberviolence). MediaSmarts’ data suggest that this trend is relatively small among youth surveyed, though the practice increases with age and is also gendered. The finding around lack of relationship between sexting and online meanness suggest that it is important to think about cyberviolence online as its own phenomena, rather than something that is “caused” by sharing intimate images. Additionally, the finding around lack of relationship between household rules and likelihood of forwarding sexts suggests that any code of conduct/guide for respect online needs to be directly linked to behaviours not considered acceptable (e.g. non-consensual sharing of photos, rape threats, homophobic slurs).

Threats Online (Steeves, 2014a)

• Thirty-one percent of students report that someone has threatened them online.
  o The majority of these students report this is a rare occurrence (once a year or less).
  o Nine percent of these students report receiving online threats on a regular basis (once a month or more).
  o The majority of the students (70%) who report receiving threats once a month or more do not see them as a serious problem.
  o One third of students who receive online threats once a month or more – three percent of the total sample – report that these are sometimes, or often, serious problems for them.
• When grade and gender are taken into consideration:
  o Boys and older students are more likely to make online threats.
  o Students in younger grades are most likely to report that online threats are often or sometimes a serious problem for them, peaking in Grade 5.
  o Girls are twice as likely as boys to see online threats as a serious problem.

Best Practice: These findings point to the fact that not all threats online are the same, nor are their impacts on the person receiving them. However, they also underscore that online threats are gendered, particularly for those experiencing these threats as a serious problem. It is important to learn more about the nature of threats online, as well as the contexts of threats experienced as a serious problem. For creating materials for social media companies, personal narratives/anecdotes of the impacts of cyberviolence might be one potentially impactful or powerful tool.
Encountering Racist and Sexist Content Online (Steeves, 2014d)

- For many students, seeing racist or sexist content is a frequent online occurrence. Over three quarters (78%) of students in grades 7-11 report that they have come across racist or sexist content online.
  - Over one third (37%) of all students in grades 7-11 see racist or sexist content online at least once a day or once a week.
  - Frequent exposure is even more prevalent among older students. By Grade 11, more than half of students (56%) report seeing racist or sexist content on a weekly or daily basis.
- Older students are more likely than younger students to encounter racist or sexist content: the percentage rises from 63 percent in Grade 7 to 88 percent in grades 10 and 11.
- Although a large majority of students agree that it is important to say something so people know racist and sexist talk is wrong (78%), just under half of students (45%) report that they feel that it is not their place to say something when it does occur.
- Older students are less likely to feel that it is their place to say something to challenge the comments.
- Gender plays an important role in this regard: Girls are more likely to be concerned about racist or sexist comments, while boys are more likely to see them as innocuous.
- Close to one-third of students in grades 7-11 (31%) report wanting to learn how to deal with racist or sexist online information.

**Best Practice:** These findings underscore the importance of paying attention to sexism, racism, homophobia, and transphobia online. In particular, they highlight a need for tools around bystander intervention; that is, talking about how to speak up against online violence and how to encourage others to do the same. In terms of potentially developing a code of conduct for online activity, identifying myths, stereotypes, words, and expressions frequently associated with racism and sexism (as well as homophobia, transphobia, and ableism) could be a valuable pursuit. The finding that older students are less likely to feel that it is their place to say something to challenge sexism and racism points to a need to talk about why that might be the case.
**Part 1: Cyberviolence: What it is and what do we know?**

This project detaches cyberviolence from the broader term “cyberbullying”. Cyberbullying has been critiqued for being broad and failing to adequately capture the gendered, racialized, and sexualized nature of much online abuse (Fairbairn, Bivens, & Dawson, 2013). It is a term that has had enormous attention in recent years. For example, a search for “cyberbullying” in ProQuest databases yields over 19,000 articles published since 2010. Many of these focus on teenagers and schools, and there is great variation in how cyberbullying is operationalized. Because of the de-gendered nature of this literature, its focus on children and teenagers, and the wide variation of behaviours studied, this broader body of work is not the focus of this inquiry.

Instead, given the specific focus of this project on cyberviolence against women and girls, the report focuses on this area. “Cyberviolence” is a less used term. For example, a search for the term “cyberviolence” in the same database yields just 143 articles and/or news stories, and a majority of these are news articles about the Status of Women project funding for these cyberviolence projects. There are 29 academic articles using this term, many from the early 2000s, when cyberviolence seems to have been more popular in the literature.

When talking about cyberviolence, we are talking about a spectrum of behaviour (Bluett-Boyd et al., 2013). Because there is not a legal understanding of cyberviolence, it is generally defined in relation to several specific acts. As mentioned, cyberviolence goes by many names (online harassment, online sexual violence, online misogyny, revenge porn, etc.). What is consistent is the gendered and sexualized nature of much of the abuse. However, many mainstream studies in this area do not focus on gender or sexuality per se. For example, MTV’s (2011) digital abuse study “A Thin Line” found that more than half (56%) of youth surveyed said they have experienced abuse through social and digital media. This rate had increased from 50 percent in their 2009 survey. No gender breakdown of this data was provided.

Additionally, when talking about cyberviolence, we are focusing less on using the Internet to commit so-called real world or physical world violence (e.g. human trafficking, Internet luring of minors for sexual assault), and more on the harms caused in online spaces. This means that we are not thinking about violence as something that is only or even primarily physical, but as something that does psychological and emotional harm to those who experience it. Yet it can also lead to physical harm, for example, through self-harmful or suicidal behaviour, and/or by adding another layer of harm or abuse to previous offline violence (e.g. sexual assault).

In recent years, four categories of cyberviolence have received the most attention in literature: online sexual harassment (including sextortion); so-called revenge porn or non-consensual pornography/non-consensual distribution of intimate images; recording and distribution of sexual assault; and cyberstalking/digital dating abuse. Each is briefly discussed below.
Online Sexual Harassment

Online sexual harassment can be thought of as gender harassment, unwanted sexual attention, and sexual coercion (Barak, 2005). The gendered nature of online sexual harassment is clear from research. For example, one study of 434 Kentucky middle and high school students found that 44 percent of the women surveyed had been victims of online harassment in the previous twelve months, compared with 26 percent of male respondents (Bossler, Holt, & May, 2012). More recently, the Pew Research Centre’s 2014 survey found that age and gender are most closely associated to experiences of online harassment. In this survey, 70 percent of young adults ages 18-24 are more likely than any other demographic group to experience online harassment, and young women ages 18-24 experience certain severe types of harassment at disproportionately high levels (Duggan, 2014). For example, 26 percent of young women surveyed have been stalked online, and 25 percent were the target of online sexual harassment (Duggan, 2014).

As Barak (2005) explains, gender harassment can be thought of as four categories in the context of the Internet. First, active verbal harassment such as gender-humiliating comments (e.g. “go make me a sandwich, bitch”), sexual remarks, so-called dirty jokes, and so forth. In active verbal harassment, there is a clear target of the harassment. Recent literature has identified rape threats as a form of online violence against women, where when a targeted person (frequently a woman) is the victim of constant messaging containing threats of sexual assault, either from a single harasser or from a more mob-style attack (Halder & Jaishankar, 2011). Online rape threats are rarely explored separately from other types of gender harassment, and there is a need to know more about the context and effects of these acts on the individuals targeted (Fairbairn, forthcoming).
Online sexual harassment can also be *passive verbal harassment*, such as “nicknames and terms attached to a user’s online identification or to personal details that are clearly considered offensive” (Barak, 2005, p. 79). Next, there is graphic based harassment, which can be *active graphic harassment* (intentional sending of graphic sexual material to individuals without their consent). Finally, *passive graphic harassment* (posting graphic sexual material to places where users have not chosen to view these materials and/or do not know in advance to expect them. Pop-up windows and being redirected to pornography sites without warning are examples of this.

In contrast to gender harassment, **unwanted sexual attention** usually involves direct personal verbal communication between a harasser and target. Messages or questions about an individual's sex organs, sex life, other intimate subjects, or other sexual invitations or insinuations are the focus here. Unwanted sexual harassment is both a) intended to gain sexual cooperation of some sort (either virtual or in face-to-face), and b) is uninvited and unwelcome (Barak, 2005).

Finally, **sexual coercion online** involves using online tools to exert pressure on an individual to elicit sexual cooperation. This coercion might involve explicit threats to harm the victim, their family, friends, or pets, harassment such as taking over or flooding emails and/or social media accounts, or even using bribes and seductions as incentives/bait to encourage sexual cooperation (Barak, 2005). Sexual coercion can be related to so-called revenge porn or non-consensual pornography/non-consensual distribution of intimate images in that the abuser in this situation can use intimate material (often initially obtained consensually) to blackmail or to engage in “sextortion” by threatening to expose a person who has shared sexually suggestive material online if they do not comply with their demands (e.g. to prevent them from breaking up with them, to force them to engage in additional sexual acts, etc.) (Comartin et al., 2013).

**Non-Consensual Sharing of Intimate Images (often called Revenge Porn)**

The term revenge porn has gained significant attention in recent years (see Citron, 2009; Salter, 2013). Revenge porn is generally described as the practice of someone (usually a man) sharing intimate photos in order to humiliate an ex-partner (usually a woman) (Citron & Franks, 2014). Because of widespread media focus and the frequent sensationalization of revenge porn, it is important to refocus this term as sexual violence (Fairbairn, forthcoming). Additionally, because young women’s social status has historically been closely tied to chastity and modesty, women are particularly vulnerable to humiliation when their private sexual life is made public (Salter et al., 2013). Since most media and academic attention to date has been on high profile cases of revenge porn, we know less about non-consensual sharing of photos as a more widespread practice involving larger peer groups. We also know little about how sexting and online sexual expression is a healthy and valued part of young peoples’ experience. Sexting refers to the use of technology to send or receive sexually explicit messages and photos, or ‘sexts’ (Comartin, Kernsmith, & Kernsmith, 2013). According to one of the more high-profile studies, one in three 14 to 24 year olds in the U.S. have engaged in some form of sexting (MTV and the Associated Press, 2011).

To date, mainstream discourses on sexting have taken a “don’t do it” approach that emphasizes individual safety strategies and responsibilization narratives (e.g. “Respect Yourself”) (Karaian, 2012; Bivens and Fairbairn, forthcoming). It is important to distinguish between sexts that are
exchanged consensually and sexts that are exchanged because someone is pressured, coerced, or threatened (Fairbairn, Bivens, & Dawson, 2013). One U.S. study involving men and women 18 years of age and older found that two-thirds of youth sending sexts had been pressured by another person to do so at least once (Comartin et al., 2013).

‘Viral sexting’, which refers to the uncontrolled spreading of sexts via cell phones and social networks, often appears to be accompanied by verbal harassment of peers and others (Comartin et al., 2013). However, given the degree of sensationalization and moral panic that sexting has garnered in recent years, it is important that a gender analysis of cyberviolence recognize the gender-double standards inherent in socio-legal responses to sexting (Bailey & Hannah, 2011), and that a youth-centered approach start from a place of recognizing that youth have sexual agency (Karaian, 2012). One way to do this is to view sexting as media production (Hasinoff, 2013), and to explore themes of consent, privacy, and safety in this context.

**Best Practice:** We need to shift away from the term revenge porn to explore how consent is practiced for youth and where support is needed. We also must learn about the factors that affect decisions about who, when, and how they express sexuality online and/or share sexually explicit material. Do young people’s definitions of sexting match up with the current best practices? What are some of their positive and negative experiences online? What kind of advice resonates around sexting for young women?

**Recording and Distribution of Sexual Assault**

An additional area that relates to non-consensual sharing of intimate material is the recording and distribution of sexual assault through social media. Recent cases in Canada and the United States, including the now infamous Steubenville case and the suicides of 17-year-old Rehtaeh Parsons and 15-year-old Audrie Pott (both of whom had images circulated of their sexual assaults) have resulted in growing awareness of the pain and suffering experienced by survivors of sexual assault, and the re-victimization that occurs through having their assaults shared through social media (Fairbairn, Bivens, & Dawson, 2013). In some cases, young women such as 16-year-old Jada Pose have taken to social media to speak out after images of their sexual assault were made public online. Legally, the distribution of images of sexual assault has been more often approached as a privacy infringement issue, rather than along a continuum of sexual violence (Powell, 2010).

**Best Practice:** Organizations should compile resources in terms of what immediate community supports are available to someone who has been sexually assaulted to help manage digital abuse and backlash (e.g. slut-shaming gossip, someone is sharing an image of an alleged sexual assault). It could be useful for organizations to also consider what forms of bystander intervention/support mechanisms can take place within these interventions.
Cyberviolence

**Cyberstalking and Digital Dating Abuse**

Cyberstalking is often discussed as a form of intimate partner violence, when a current or former spouse or partner uses online technologies to threaten, harass, track, or control the victim. Some research notes that cyberstalking seems likely to increase in prevalence as various technologies (e.g. social networking sites, global positioning systems) become more and more pervasive in day-to-day life (Nobles et al., 2012). Additional research has documented the ways that domestic abusers use social networking sites to intimidate and monitor their current or former partners (e.g. Baughman, 2009; Belknap Chu, & DePrince, 2012).

Among youth, digital dating abuse is a relatively new term being used to describe similar patterns, where one partner in a romantic relationship uses social media and/or other technologies (such as cell phones) to control or harass the other (Picard, 2007; Weathers, 2012). However, we do not know a great deal about how young people use online tools to abuse, control, and harass people they are dating and/or romantically involved with, and/or how young people experience what is sometimes called cyber dating abuse (Zweig et al., 2013) or digital dating abuse (Weathers, 2012).

**Best Practice:** Much research on domestic violence focuses on physical abuse. In exploring youth relationship abuse and social media, focus on how power and control take place in social media, and what youth perceive healthy relationships to look like. Organizations should consider drawing from the Canadian Women’s Foundation’s #HealthyRelationships material to see if this list of criteria reflects young women’s perspectives in their communities.

**Best Practice:** In light of research on the promotion of dating violence in mass media content (Manganello, 2008; Collins and Carmody, 2012), we must expand the focus on cyberviolence to find out what types of mass media content may be most significant for the formation of ideal and healthier romantic relationships.

**Other Forms of Cyberviolence Young Women are Talking About!**

*Through our conversations with young women in Ottawa, as well as what we already know from our process of inquiry, OCTEVAW’s Youth Advisory Committee (YAC) decided that it was important to acknowledge the lesser known forms of cyberviolence and issues young women are experiencing and negotiating here in Ottawa.*

**Online Hate (sexism, racism, homophobia, transphobia, ableism etc.)**

The Internet has been rightly hailed as a groundbreaking interactive centre of ideas where anyone with access to software and smartphones can participate. It has become an essential means for

---

1 In practice, cyberstalking can include activities such as: monitoring email communication directly or through spyware or keystroke logging hardware; sending messages intended to threaten, insult, or harass; disrupting online communications by flooding a victim’s online accounts with unwanted messages or by sending a virus; using the victim’s electronic identity to send false messages to others or to purchase goods and services; using online sites to collect a victim’s personal information and whereabouts (Baughman, 2009).
young people to access information, services and community but the downside of this unparalleled information exchange is that, alongside its many valuable resources, the Internet also offers a host of problematic materials – including hateful content – that attempt to harm and undermine certain groups of people. Though the line between free speech and hate speech is a thin one, it’s a conversation worth having. Many young people, particularly young women and other marginalized genders are particularly concerned about the affects of racism, sexism, homophobia and transphobia online. Though not much exists in terms of research regarding this particular issue young people understand the gendered impacts of violence online and want us to know that young women & girls are being targeted because of their gender expression (Mediasmarts, 2015).

“We need to continue discussing online violence. We need to discuss the impacts but also the need to talk about how young people, especially us girls & queers, are taking ownership of these spaces. I am sick and tired of seeing rape myths and problematic gender norms online. I am tired of seeing my friends getting hurt or targeted just because of their gender or sexuality. I am tired of people thinking that it’s not a big deal. It hurts and it’s just as real as offline life. It’s not because people are mean, it’s bigger than that.”

(Member of the PSYAC at YSB, 2015)

**Cyberharassment (trolling, flaming, dogpiling, chaining, false flagging etc.)**

The notion that cyber harassment is trivial is both widespread and damaging. Because so many refuse to recognize cyber harassment as harmful, women suffer in silence, often sacrificing their identities and their online lives (Keats Citron, 2009). Cyber harassment is the use of social media and online spaces to harass, control, manipulate or coerce women and other marginalized genders online. Unlike physical harassment involving face-to-face contact, cyber harassment requires the use of social media and is verbal, sexual, emotional or social abuse of a person, group or organization. The cyber harasser’s primary goal is to exert power and control over the targeted victim. *Adapted from Women, Action & Media’s Twitter Report (2015)*:

**Trolling & Flaming**

Trolling and flaming are online harassment techniques often used in various online forums. These occur on social media sites, personal blogs, chat rooms, email groups and famous video sites such as YouTube. Harassers engaging in trolling or flaming tactics often use social media to intimidate, insult and confuse people because they can remain anonymous. Trolling is a phenomenon that has swept across websites in recent years. Online forums, Facebook pages and newspaper comment forms are bombarded with insults, provocations or threats. Supporters argue it's about humour, mischief and freedom of speech. But for many the ferocity and personal nature of the abuse verges on hate speech.

The flamer writes content that will invoke certain emotions and responses such as rage, sadness, humiliation, self-doubt and more. Some flamers seek out people who are enthusiastic about certain subjects, and they intentionally bash the subject. Some flamers intentionally start arguments about any topic. Most of the time, they have no valid reason for arguing, and they will often get defensive if anyone challenges their flames. The second email or comment from a flamer usually involves profanity and personal insults. Flamers often target someone’s race,
gender, sexual orientation, economic status and more, which leaves young women and other marginalized genders particularly vulnerable to this type of online harassment. If the flamer can find out any personal information about a target, then they will use it to cause that person harm and distress. Negative responses fuel flamers the most because they know that they have upset other people.

_Dogpiling_
This is a type of online harassment stemming from multiple accounts at the same time as part of a campaign or coordinated attack. Young women and girls are particularly subjected to this type of harassment. They’re receiving—and receiving and receiving—threats and insults. This is high volume harassment. Consequently, filing a new report for each harassing account becomes an extension of the harassment, something harassers are aware of. A person who experiences dogpiling needs to be able to take action on—and collect evidence on—multiple accounts at the same time (WAM, 2015).

_Chaining (or account suspension evasion)_
This type of harassment is perpetrated by a single individual or few individuals, where the harassing accounts are regularly suspended only to be replaced by new ones run by the same harassers (suspension evasion). Forms of online harassment involving a linked series of accounts. A person experiencing chaining needs to be able to link harassment reports together and for social media platforms to catch, prevent, and take action on harassers’ chaining patterns. These are typically easily recognized as violations of platform’s terms of service and rules, and reporting them leads to account suspension. Harassers then open new accounts and begin their practices again. Key to this process is signaling to the target of harassment that a new account is related to one that was suspended. This is often achieved through use of a similar account name, recognizable profile details, or explicit boasting of continued presence despite suspensions. This signaling is a critical point of intimidation—but also opens a potential point of intervention (WAM, 2015).

_False Flagging_
When a person uses a social media platforms harassment reporting process to attempt to silence or intimidate an account. This expends valuable resources of report and review mechanisms on social media platforms.

_Doxxing (releasing private information)_
_Doxxing_ refers to the search for, and subsequent publication of private (non-public) personal information of people and their identities. Specifically, the names, numbers, residences, etc. of users on anonymous sites and platforms who aren't figures of entertainment, sports, politics, or other public media, as well as their friends, family, children and associates.

People are ‘doxxed’ maliciously more often than not and often the goal is to ‘seek revenge’ or to 'punish' the person for ‘something they did’. It can escalate from fairly minor and childish pranks, to attempts at costing the person their job, harassment of friends/spouses/family members.

_Multiplatform Harassment_
This type of harassment online is part of a larger trajectory of harassment that moves and builds across multiple platforms. This involves threats, insults, and other unwanted contact directed toward them via channels such as social media accounts, email, blogs, professional presence (online and otherwise), and telephone. Harassment may come from a single individual or a group. Harassers follow, friend, and contact people this person knows, and use the person’s online presence to stalk and/or publicly humiliate them. Harassers may also be impersonating the individual on other platforms and inciting others to attack them. This is a multi-headed monster; individual platforms can only address the issues that they see, and addressing this harassment as separate instances may obscure the larger context of harassment this person is experiencing (WAM, 2015).

“Outing” & Exploiting Vulnerabilities Online

When LGBTQ people are first coming out, they are very vulnerable to sexual violence abuse - they may be losing friends and family, may be alienated from their cultural, ethnic, religious, familial community and institutions. The isolation that most LGBTQ people face as a result of homophobia and transphobia is useful to a perpetrator who is trying to isolate them. Threatening to “out” a person (which could mean losing children, ostracism, job loss etc) is a powerful tool of control, especially in an online context. Similarly, a perpetrator may target and exploit someone’s identities, experiences and vulnerabilities to obligate or coerce someone. Using vulnerabilities and outing often results in survivors being exploited (resources, time, attention) and undermines their attempts to negotiate boundaries and access self-determination. For example, a person may target someone because of their identity as an LGBTQ person or because they are someone living with mental health issues, etc. Often times people who are depressed or suicidal may be targeted and exploited online (Burke & Tucker, 2009).

Impersonation & Identity Theft

Impersonation is when a person online pretending to be someone else and sends or posts material to harm a person and damage their reputation or friendships. A person may create a fake profile in your name in order to harass, intimidate, threaten or defraud another person. Consequently, there are multiple ways in which impersonation and identity theft can perpetuate cyberviolence. One way is when an account is made in the victim’s name and used to say compromising or inappropriate things in their name. Another way is that the abuser uses the victim’s name to gain the confidence of their friends in order to learn private things about them.

Summary:

The above section has provided an overview of cyberviolence against women and girls and has highlighted some knowledge gaps and potential recommendations and best practices. It also highlight some of the emerging issues that young women in Ottawa are talking about that often get left behind in academic research. Research on cyberviolence has primarily focused on individual and psychological characteristics of those experiencing or perpetrating abuse. Additionally, most academic research of youth and cyberviolence has focused on earlier social networking sites such as MySpace, Facebook, and Twitter, leaving out a many popular social media spaces identified by young women which is why it is important to incorporate emerging issues highlighted by media coverage of cyberviolence in our needs assessment process.
**Part 2: Emerging Issues Highlighted by Media Coverage of Cyberviolence**

As previously mentioned, we know that peer reviewed academic research tends to lag behind emerging phenomena due to publication timelines. It is therefore important to look to news stories for information about evolving and emerging social media sites and apps, as well as to continue to explore from young women in Ottawa what platforms are most interesting, most important to them, and how their sense of well being varies by platform. To contribute to the objective of this project, this next section explores news coverage of cyberviolence against women and girls to get a sense of high profile cases and specific platforms that are at the center of current debates and discussions around cyberviolence. These tend to center around four main themes: harassment of sexual assault survivors; hookup culture, sexuality, and online dating; anonymity and cyberbullying; and sexualized and gender violence as entertainment.

Before delving into news coverage of cyberviolence, it is important to note that there are many news articles on social media sites and sexual violence that focus on how social media is being used to connect survivors (for example, the #BeenRapedNeverReported Twitter hashtag in 2014) (Teotonio, 2014), to discuss sexual violence more broadly (for example, in relation to the Jian Ghomeshi case currently before the courts), and/or prevent violence through digital innovations (see Apps Against Abuse, Businesswire, 2011). Young people’s experiences, and social media, are often portrayed as trivial and/or stereotyped in other ways by older generations, who often hold more power in society generally to construct these narratives. As such, in considering news coverage of cyberviolence it is important to acknowledge that while young people’s work in violence prevention (and social media’s role in this work) is not the focus here, they are nonetheless important to acknowledge.

**Harassment of sexual assault survivors**

News stories about sexual assault frequently elicit cyberviolence in the form of hateful online commentary. For example, last fall *The Toronto Star* published an opinion piece on the need to protect sexual assault victims from domestic abuse, after sexually violent comments were made towards a survivor within the Star Facebook page (English, 2014). News outlets generally do not have the capacity to monitor all comments and may therefore shut down comments on the news pages of violent crime stories. However, they do not have the ability to shut down social media comments shared about news stories, and survivors therefore may face high risks of harassment when they agree to be interviewed in news stories.

**Implication for OCTEVAW:** Post the recently developed Survivors Media Guide (CounterQuo, 2015) to OCTEVAW’s Media Hub, and consider holding a workshop or focus group to discuss the guide with youth who identify as survivors of violence.

Three high profile cases of online harassment of sexual assault survivors are the Steubenville case and the experiences of Rehtaeh Parsons and Jada Pose. The widely publicized events of Steubenville took place on August 11, 2012, when a 16-year-old girl, who was alternating between unconscious and barely conscious and vomiting, was dragged around various parties and repeatedly sexually assaulted (Gwynne, 2013). Various people, including at least two
Steubenville high school football team members, who were later charged in the case, documented the assaults through Twitter comments and photographs.

Rehtaeh Parsons was a 17-year-old Nova Scotia high school student who committed suicide after a year and a half of online abuse after being sexually assaulted in November 2011. She died on April 7, 2013. Her case has been highly influential in Canadian advocacy and policy arenas, and Rehtaeh’s father, Glen Canning, has become an advocate for preventing sexual violence and advocating for reforms around cyberviolence.

Finally, Jada Pose is a young woman (16 years old at the time of the assault) who was sexually assaulted and then had pictures of her naked body posted to social media. Here, she was harassed by users mocking and imitating her using the hashtag #jadapose (Collman and Warren, 2014). Jada spoke out about her abuse to mainstream media and received a great deal of support through social media campaigns.

One narrative common to these cases is the perception that alcohol is a cause of sexual assault (rather than a tool, or a weapon). In an additional case from California, 16-year-old Audrie Potts committed suicide after young men circulated images sexually assaulting her. Some news media described this case as “as yet another example of the dire consequences of teenage drinking, risky behavior and a camera in every pocket” (Sulek, 2014, para 5). Such framing is problematic for facilitating victim-blaming and sexual assault myths, as well as the idea that technology causes violence.

We know little about the many cases of sexual assault that do not make the news, and about the nature and extent of cyberviolence that survivors face. This is an important area to explore, particularly because we do know that sexual assault survivors are frequently blamed and shamed for the violence they experience in other mediums. Exploring the role of bystanders in standing up to victim-blaming and shaming is a particularly important area.

Implication for OCTEVAW: Continue to work with youth to further develop a definition of cyberviolence and incorporate this into strategy development. Young women in Ottawa are talking about cyberviolence in many different ways. The most common terminology we have found in speaking with young women is the use of the term cyberharassment, as well as cyberviolence. Additionally, young women seem to identify best with the term cyberharassment because they feel like it really captures the sustained and ongoing harassment and violence they face online and offline. While no single definition of cyberviolence was agreed upon, the young women really stressed the gendered impact of cyberviolence. Young women in Ottawa want us to know that cyber and sexual violence have to do with being women and girls online and that we need gender to explicit in our conversations. Young women and young LGBTQ people in Ottawa are being targeted more frequently and with greater impact than young men online and this must be a key focus of this project.

Implication for OCTEVAW: Throughout our development process we looked to find out more about online supports available to survivors of violence, and what factors are associated with them being able to seek out these platforms (or not). When reaching out to engage social media companies, we needed to consider exploring the question: “When someone is sexually assaulted,
what can your company currently do to prevent them being identified and harassed online?”
This question has laid the groundwork for engaging with social media companies and the tech sector in Ottawa.

**Hookup culture, sexuality, and online dating**

In mainstream media discussions around youth, social media, and sexuality, there is a preoccupation with so-called hook-up culture and its links to sexual assault and cyberviolence (Guarino, 2013). These discussions frequently centre on dating apps and their role in facilitating or enabling what is often framed as promiscuous or high-risk behaviour. This is a notion that needs to be critically explored and problematized within cyberviolence, as stigma about young people having sexual relationships involving multiple partners is a barrier to prevention of sexual violence.

The issue of younger teenagers using dating apps has received some media attention as an area of concern. For example, a recent survey by ChildLine of 400 youth under sixteen found that more than a quarter of children use specialist teen dating apps, as many as 29 per cent admitted they had been in touch with someone over the age of 18. Of those, 72 per cent said the person who contacted them online had known their real age (Philby, 2014). Because OCTEVAW’s cyberviolence project focuses on 16-24 year olds, 13-16 year olds are likely not a central group of attention. However, it may be important to be aware of the experiences of young people with online dating apps and to potentially explore how these experiences can help to inform cyberviolence prevention.

In terms of older teenagers and young adults, Tinder has received significant attention as a dating and hookup app. Tinder uses GPS technology and gathers basic information to match people in the same geographical area may be compatible. In Australia and New Zealand, there has been a fair amount of attention to the links between online dating and sexual assault involving Tinder, after high profile events of sexual violence (Hume & Day, 2014). In one event, a New Zealand tourist was gang-raped after meeting up with a man she met through Tinder. In another, a young woman died after falling off the balcony of a man whom she met on Tinder. Conversations about these events focus heavily on the role of social media rather than factors related to sexual violence more broadly. Some media coverage characterizes sexual violence as due in part to the superficiality/speed of social media. For example, one article, quoting a clinical psychologist about the role of social media in the balcony death of the young woman, said:

> Online dating sites, including Tinder, are romance on speed - a shortcut, she says. People could message after the initial physical introduction and go on a date straight after that. She warns people to be sensible - and aware of dangers. "People using Tinder are bold and do not mess around. They move more quickly to the 'hey babe, can I have your number' stage," she says. Tinder is based on physical attraction, which could lead to different expectations." When there is a clash in expectations, it can lead to trouble. If one person is naïve and the other predatory, it can have a nasty outcome. "People have to be super careful of this behaviour. Someone pressuring you is not good." (Devlin & Daly, 2014, para 6).
Young women are frequently framed as risk taking and naïve when it comes to their social media use. For example, the article above opens with “The death of Lower Hutt 26-year old Warriena Tagpuno Wright in Surfers Paradise exemplifies the risks women put themselves at when meeting strangers.” There are some sites that present safety advice for young women using dating apps. This advice includes advice such as: meet in a public place; tell friends where you are going; arrange your own transportation; don’t drink too much; take it slow; consider a double date; trust your instincts; and research the person you are meeting (Healy, 2014). This is similar to much individual safety strategy sexual violence prevention advice that keeps the focus on young women to protect themselves from sexual violence.

More recently, a number of woman-centric dating apps (Wyldfire, Mesh, Singled Out, Bumble, Lulu and Siren) have emerged that have a number of mechanisms designed to give women more control over their online dating experience (Zuniga, 2015). These apps position women as gatekeepers by giving them increased control over who sees their profile, who can contact them, and even by filtering out graphic photos and curse words in one case (Mesh) and allowing men to join only based on recommendations and invitations by female members (Wyldfire). One idea for further needs assessment and programming design could be to workshop these various dating apps to explore their pros and cons for young women, and perhaps even engage with their creators.

Implication for OCTEVAW: Consider workshopping woman-centered dating apps with young people to find out what works for them within these apps and why. These findings could potentially be shared during the knowledge sharing and strategy phases with social media companies who are willing to commit to working on sexual violence prevention within their platform.

Anonymous and online harassment

In addition to dating apps, various platforms that encourage anonymous posting and commentary have garnered international attention, in part due to their role in cyberbullying and online harassment and their links to suicides of young women such as Amanda Todd, Hannah Smith, and Jessie Logan. They are also linked to death threats, rape threats, and sexual harassment experienced by feminists online (see Lalonde, 2014).

One of the most well known anonymous posting websites is 4chan. 4chan is an image-based bulletin board where anyone can post comments and share images, and do so anonymously. Two high profile cases of cyberviolence related to 4chan are the 2010 harassment of Jessi Slaughter and the 2014 distribution of celebrity nude photos. In 2010, members of 4Chann began to harass 11-year-old Jessi Slaughter after a user said she was having a relationship with an older man. Users posted her address, called her house, and spread false rumors and reports about her and her family. The harassment was so severe that the young girl was put in police protection at one point (Klausner & Warren, 2015).

---

2 What is 4chan? https://www.4chan.org
In 2014, what many mainstream media outlets called the “Celebrity Nude Leaks” involved Anonymous members of 4chan and reddit stealing and distributing hundreds of nude photos of celebrities, eventually leading the FBI to get involved (Klausner & Warren, 2015). Millions of people viewed these photos. However, there was also a conversation about non-consensual sharing of intimate images as sexual violence that happened, as many made the connections that sharing and viewing these photos is sexual violence (Cheney-Rice, 2014). Although many of the highest profile news stories of non-consensual distribution of intimate photos have involved celebrities, having nude photos leaked online is not exclusive to celebrities. For example, in 2010 the husband of a Manitoba judge posted intimate photos of her online. The judge is currently set to face a disciplinary panel to determine whether the photos are “inherently contradictory to the image and concept of integrity” of the judiciary (Canadian Press, 2014).

In terms of application-based platforms that allow for anonymity, Twitter is the most high profile and widely used messaging platform generally, with 288 million monthly active users worldwide. Although many users are not anonymous, Twitter has come under scrutiny in recent years for its failure to adequately respond to and prevent gendered and sexual harassment in its platform. For example, some high profile cases include: death threats and sexual harassment towards feminist media literacy critic and gamer Anita Sarkeesian and her family (Ryan, 2014) as well as Gamergate more broadly (Hathaway, 2014); rape and death threats towards Caroline Criado-Perez, who campaigned to have women on England’s banknotes (Kennedy & Hamilton, 2013); and threats towards UK Member of Parliament Stella Creasy, who stood up online for Criado-Perez (Murphy, 2013). Twitter has recently entered into a partnership with the organization Women, Action, & the Media (WAM!) to work to more easily report and respond to gender harassment online (Women, Action, & The Media, 2014).

In addition to Twitter, there are a number of additional apps where anonymous online harassment has received media attention. Perhaps most prolific is Ask.fm, launched as a social networking site in 2010 and based around anonymous posting (the anonymous question and answer section has been particularly controversial). By 2013, its user base was more than 60 million. This same year, the British prime minister called for a boycott after reports that cyberbullying there had contributed to several teen suicides (Van Dusen, 2014).

YikYak is a “virtual bulletin board” that allows anonymous users to post and view 200-character messages within a 10-mile radius of one another. According to one article, “it isn’t just anonymity, it’s local flavour” (Teitel, 2014, para 5). Other so-called “confessional apps” (Streetchat, Whisper, Topix, After School, and Secret) similarly rely on anonymity to various extents. Some, such as Whisper, purport to be fully anonymous, where users can make a statement (confession) and/or ask others a question to which they can respond. Others, such as Secret, include the user’s neighborhood when they post, or are linked to a particular school. In December 2014, an app called After School was pulled (for a second time) from the App Store following a post that read: “Tomorrow I’m gonna shoot and kill every last one of you, and it’s going to be bigger than Columbine . . . Death to you all” (Van Dusen, 2015, para 4).

In terms of OCTEVAW’s project, once youth advisory committee/project partners have created a working definition of cybersexual violence, OCTEVAW could consider exploring youth

---

3 Twitter “About”. https://about.twitter.com/company
experiences in these apps to identify examples of cybersexual violence. OCTEVAW could work
with local partners (e.g. Draw the Line campaign) to come up with scenarios to identify and
respond to cyberviolence in anonymous, location-based apps. What reporting mechanisms exist
for cyberviolence through location-based apps? As an example scenario: “If someone reported
they were going to ‘get someone drunk’ that night and ‘have sex with them’ and the post was in
your neighborhood, what could you do?”

**Implication for OCTEVAW:** A strategy development idea identified throughout our needs
assessment process is to explore the option of working with a partner such as Hollaback! or Take
Back the Tech to report and map cyber violence in particular apps. These pilot reports and
findings could be shared with community partners and/or social media companies to report abuse
cases.

**Gendered and sexualized violence as entertainment**

A final area of cyberviolence that has received news coverage attention in the last few years is
the creation and sharing of gendered and sexualized violence on social media as jokes or
entertainment. This is often linked to the concept of rape culture or normalization of rape (Kane
& Marco, 2013) where attitudes tolerant and supportive of sexual assault are embedded in
various facets and levels of society (norms, attitudes, policies, media content, and so forth).

In recent years both Facebook and Twitter have been the target of large-scale, collaborative
feminist media campaigns that aimed to pressure these companies to address Facebook “joke”
pages promoting violence against women (e.g. “how to rape” and “joke” domestic violence
pages) as well as the harassment of women on Twitter. These campaigns have been successful in
starting partnerships with social media companies. The organization Women, Action, & the
Media announced partnerships with Facebook in 2013⁴ and with Twitter in 2014⁵ to address
online violence.

**Implication for Practice:** Consider creating a violence prevention communications policy with
which organizations could be “stamped” or “accredited”. This would reflect a commitment to
preventing misogynistic, racists, and/or homophobic speech. It would not have to necessarily be
directed at large scale social media platforms, but could be initially targeted to local businesses,
organizations, or media outlets, for example, to commit to keeping their online spaces violence-
free.

In Canada, a case that has garnered national attention involves the so-called Gentlemen’s Club
Facebook page of Dalhousie Dentistry students. This page involved “offensive and misogynistic
exchanges on Facebook including a poll in which they voted on the female students they would
most want to have “hate” sex with” (Taber, 2015, para 1). This case has started conversations
around many themes, including the role of bystanders online. This further builds on local

---

⁵ Women, Action & the Media, November 6, 2014. “To combat the harassment of women online, Women,
Action & the Media (WAM!) announces a new partnership with Twitter”. Press Release.
conversations in Ottawa that took off in 2014 when a University of Ottawa student leader was the subject of sexually violence online conversation (Canadian Press, 2014).

Finally, some recent news coverage suggests that sextortion is on the rise in Ottawa, with 30 cases reported last year to Gatineau police (Hempstead, 2014). Cyberstalking has also received media attention locally, with dozens of women reporting in 2014 (Gillis, 2014).

**Implication for OCTEVAW:** During the knowledge sharing phase of the project OCTEVAW could explore with community partners at the Justice Committee what police data exists on cyberviolence in Ottawa, what young people think about it and how this could be used during the strategy development and implementation phase with the youth advisory committee.

**Summary**
Many of the platforms highlighted in news stories in relation to cyberviolence are based on anonymity. It is unlikely that social media sites will give up this feature, as it is a central draw for users. Additionally, because there are new social media sites and applications coming out all the time, it may not be highly effective to specifically target a particular app or site for cyberviolence prevention. Instead, it is likely more effective to focus on what elements of cyberviolence are common to various platforms, and see if there is a preventative mechanism that can be built in there instead. In this way, there may be possibilities and opportunities to work with social media designers who would consider implementing policies where users’ anonymity can be removed if it is abused. (For example, if a rape threat is made or certain misogynistic or racist language is used).

While the cases highlighted by these news stories demonstrate cyberviolence is a problem, because news media tend to focus on the more extreme or sensational cases, the nature and extent of cyberviolence in the everyday lives of young people is less clear.

News stories also underscore a need to develop reporting and bystander intervention approaches. Concrete strategies for what to do under various forms of cyberviolence (e.g. infographic/flow chart, slogans, or contact info for direct access to a support worker) might be helpful here.
Part 3: Responses to Cyberviolence

This section focuses on government, legal, and community responses to cyberviolence, as well as a brief discussion of individual risk-reduction strategies.

This process found no empirical studies evaluating cyberviolence prevention initiatives. However, there are a number of pieces that we can draw from more broadly to start identifying needs and potential actions.

Historically, recommendations for cyberviolence prevention have focused on three areas: legal, changing the organizational-social culture, and education and training of potential victims as well as of potential harassers (Barak, 2005). This section adapts these themes by considering government responses, legal responses, community responses and programming, and individual strategies. It also looks at research findings on emerging and recommended responses to cyberviolence.

Government responses

To date, Canadian policy responses to sexual violence and social media have occurred in relation to two prominent cases. On October 10, 2012, Amanda Todd, a 15-year-old British Columbia student, committed suicide following months of online sexual exploitation, blackmailing, and bullying. Less than one month later, Justice and Public Safety Ministers directed government officials to identify potential gaps in the Criminal Code of Canada on cyberbullying and the non-consensual distribution of intimate images (Department of Justice Canada, 2013). Following the April 7, 2013 death of Rehtaeh Parsons, a 17-year-old Nova Scotia high school student who committed suicide after months of digital abuse related to her sexual assault, Ministers demanded this work be expedited and requested a final report that summer (Department of Justice Canada, 2013). The final report was released in June 2013, and Bill C-13, the Protecting Canadians from Online Crime Act, was introduced in November 2013, passed by the House of Commons on October 20, 2014, and received Royal Ascent on December 9, 2014. Bill C-13 relates to cyberviolence only insofar as it targets the non-consensual distribution of intimate images. While not insignificant, it does not address other forms of cyberviolence.

Some provincial governments have also taken steps to address cyberviolence. In 2013, Nova Scotia passed the Cyber-safety Act, the first legislation of its kind in Canada aiming to protect victims of cyberbullying and hold those responsible accountable under the law (Cyberscan, 2015). According to this initiative, “instead of having to rely solely on police pursuing criminal action, victims and their families now have new civil options including seeking protection/prevention orders and suing cyberbullies for damages” (Cyberscan, 2015). CyberScan, Canada's first cyberbullying investigative unit, was developed as a result of this legislation.

Additionally, the Federal Government has distributed various resources through the Royal Canadian Mounted Police Internet Safety webpage\(^8\) and the Stop Hating Online Government of Canada page.\(^9\) However these are primarily cyberbullying resources and do not included gender-based analysis. Additionally, they are primarily geared towards children and youth under sixteen.

**Legal responses**

In 2014, West Coast LEAF produced the comprehensive report *#CyberMisogyny: Using and Strengthening Canadian Legal Responses to Gendered Hate and Harassment Online*. This report lays out 35 recommendations for Federal and Provincial governments to respond to and prevent cyberviolence. It considers various Criminal Code provisions and Torts that can be used to respond to cyberviolence, including: criminal harassment, (s. 264 (2)); extortion (s. 346), intimidation (s. 423); uttering threats (s. 264.1); voyeurism (s. 162); defamatory libel (ss. 300 and 201), and more.

As West Coast LEAF explains,

> Criminal harassment is the most frequent charge in cases involving non-consensual distribution of intimate images. Section 264(2) defines harassment as (a) repeatedly following someone; (b) repeatedly communicating with someone either directly or through another person; (c) besetting or watching someone’s home or workplace; or (d) engaging in threatening conduct towards someone or a member of their family. Subsections (b) and (d) are most relevant to cases of cyber misogyny. Importantly, the behaviour is only criminal when it causes the target to reasonably fear for their safety or the safety of someone they know. (p. 16).

This report makes it clear that legal concepts such as defamation and extortion can apply to cyberviolence. The report also clearly states that a “reasonable fear for safety” can include both physical and emotional or psychological safety, and the offence will be made out when the psychological integrity, health or well-being of the victim has been interfered with in a substantial way. (West Coast LEAF, 2014, p. 17)

Historically, challenges for preventing cyberviolence have included anonymity, the legal status of the Internet, and the cultural and social norms of cyberspace (Barak, 2005). However, recently scholars have begun to problematize the notion that the Internet is a “wild west”, free of legal responsibility (Citron, 2009). In Australia, Bluett-Boyd and colleagues (2013) produced a lengthy report exploring sexual violence online in legal contexts. In the U.S., Marwick and Miller (2014) analyze legal remedies available for online hate speech, harassment, and defamation. This report also includes a summary of state laws on online harassment. In a U.S. context, Marwick and Miller (2014) find that:

---

\(^8\) Royal Canadian Mounted Police Internet Safety webpage. http://www.rcmp-grc.gc.ca/cycp-cpcj/is-si/isressi-eng.htm

While victims may want to explore other remedies, such as appealing to content hosting platforms, there is no legal requirement for sites like Facebook or Twitter to aggressively monitor their content, remove offending messages, suspend the accounts of perpetrators, or enforce terms of service. Some sites may choose to do so, but others...[including] the hosts of so-called “revenge porn” sites, may actively resist such efforts. However, community moderation, collective norm-setting, aggressive algorithmic filtering of online comments, or other social or technical efforts may help to quell these problems (p. 27).

Although OCTEVAW’s project does not focus on legal interventions for cyberviolence, it may be worthwhile to reach out to the authors of these studies and/or the associated research centres to see if there are any resource or knowledge sharing opportunities.

**Best Practice:** Hold a workshop with a legal expert (ideally a young person) on young people’s legal rights when it comes to online sexual expression (e.g. sexting) and cyberviolence. Additionally, consider what other audiences might benefit from such a workshop.

**Community responses**

Activists and advocates have been leaders in bringing cyberviolence onto the broader social agenda. The Association for Progressive Communications’ *Take Back the Tech* campaign is perhaps the most large-scale, comprehensive, and targeted advocacy effort to currently focus on cyberviolence. *Take Back The Tech* is a collaborative campaign that takes place each year during the 16 Days of Activism Against Gender-based Violence (November 25 - December 10). It acts as “a call to everyone - especially women and girls - to take control of technology to end violence against women”.  

Additionally, there are a great deal of resources on their website, including ten tips for Challenging *Internet Based Gender-Discrimination and Online Harassment Against Women And Girls*. These tips go beyond individualized safety advice to promote a narrative of empowerment, choice, and well being, and would likely be a good starting point for a workshop about these themes in the context of cyberviolence. As such, they are included in *Appendix A* of this report.

**Implication for OCTEVAW:** During the Strategy Development phase consider a specific youth-led initiative as part of the 16 Days campaign in November, perhaps coordinating with In Love and In Danger.

In terms of other community strategies and responses, as noted earlier, feminist media advocacy group Women, Action, and the Media (WAM!) launched projects in 2014 to work with Facebook and Twitter on gender-based harassment and promotion of sexual violence. Another advocacy organization working in this area is *Futures Without Violence*, who developed the

---

11 Ten Tips for Challenging Internet Based Gender Discrimination and Online Harassment Against Women. *Take Back the Tech*.  
https://www.takebackthetech.net/blog/10-tips-challenging-internet-based-gender-discrimination-and-online-harassment-against-women
online campaign That’s Not Cool (thatsnotcool.com). This youth-focused campaign encourages teenagers to make their own decisions about developing healthy relationships through the use of videos, interactive games, and an online forum for sharing stories and advice.

There are also a growing number of community-based initiatives geared towards cyberviolence. For example, the Rehtaeh Parsons Society, created in late 2014, will provide funding for education, skills, and tools to address cyberbullying, youth sexual violence, and the distribution of images around young people (Canadian Press, 2014). Draw the Line is an anti-sexual violence campaign that has been proactive in encouraging people to start conversations about cyberviolence against women and girls, developing posters with slogans such as “A friend sends you a naked picture of a girl he knows. Is it a big deal to share it with others?”

**Individual strategies**

There are many examples of cyberviolence prevention in the form of individual safety tips and strategies. An example of such a list is provided by Rape Crisis Scotland. Tips here include:

- Never share private or identifying information when using social networks.
- Check your privacy settings to make sure you are not sharing more information than you intend. Review and reset them regularly.
- Use ‘strong’ passwords and change them regularly; don’t use the same password for different websites.
- Pick a user name that does not include any personal information or place names such as where you live or hang out.
- Keep your profile ‘closed’ and only allow your friends to view your profile.
- Be wary about who you invite or accept invitations from.
- Make sure that any ‘friends’ you make online are real ones and not just ‘friends of friends’.
- Do not send or post photographs online that you would not want anyone else to see. This includes any photographs that someone sends to you.
- Do not do anything in front of a webcam that you would not want the world to see.
- Some people may try to get you to do things you don’t want to, such as sending them an explicit photograph of yourself. They may use this to ‘blackmail’ you into doing something else with the threat that if you don’t, they will send the photograph to other people.

It is important to note here that individual safety strategies may prevent individual victimization in some cases, but there is no evidence that they stop cyberviolence more broadly. Additionally, by conveying the idea that it is up to individuals to prevent becoming targets or victims of cyberviolence, these frameworks can contribute to victim blaming and shaming (Bivens &

---

Given OCTEVAW’s project goals and focus, it is important that strategy development focus on youth-led activities to change social/online norms and social media design over a focus on individual level safety strategies. However, for those interested in a more individual, DIY approach to online safety that emphasizes data protection, the *DIY Guide To Feminist Cybersafety* an example of a resource that emphasizes more empowerment-based approaches to online safety: [https://tech.safehubcollective.org/cybersecurity/](https://tech.safehubcollective.org/cybersecurity/).

**Best Practice:** Consider using the ten tips for *Challenging Internet Based Gender-Discrimination and Online Harassment Against Women And Girls* from *Take Back the Tech* (included in Appendix A) and the *DIY Guide To Feminist Cybersafety* as conversation starter/focus group model to revise and reform individualized safety strategies.

**Technological responses**

In recent years, digital technologies have been used as prevention tools to combine social actions with digital technologies. Application based platforms (apps) like METRAC’s *Not Your Baby* app, the *Circle of Six* app, and OCTEVAW’s *RISE* app are all examples of using digital technology to target sexual violence more broadly.

Using digital tools to target cyberviolence is a less explored area. However, “Trollbusters” is an emerging platform specifically geared towards ending cyberviolence against women (Reynolds, 2015). Winner of the 2015 International Women’s Media Foundation Hackathon, the recently developed “TrollBusters” platform markets itself as “Offering pest control solutions for women publishers.”[^14] Michelle Ferrier, a former journalist who was driven out of her job by sexist and racist harassment and threats between 2005 and 2007, leads its team of creators (Reynolds, 2015). TrollBusters has three components: 1) An S.O.S. team working to counter cyberattacks in real-time with online community support and positive messaging; 2) RAID: Finding and outing trolls online and tracking where they operate using network analysis technologies; and 3) SUPPORT: Providing technical, legal, and psychological services, and resources for publishers under denial of service attacks (Ferrier, 2015).[^15] As this project evolves, it will be an imprint one to watch. A PowerPoint presentation on TrollBusters is included as Appendix B.

**Best Practice:** Review TrollBusters presentation (Appendix B) and explore possible follow-up opportunities (workshops, partnerships) at a local level.

---


Findings and recommendations

There is a growing body of research about the intersections of digital technologies and sexual violence. Existing work has focused on the prevalence and nature of online sexual violence (Citron, 2009; Bluett-Boyd et al., 2013; Salter, 2013); critically considered social and legal narratives about digital sexual expression (e.g. Bailey, 2009; Karaian, 2012; Ringrose et al, 2013), detailed the gendered dimensions and implications of online sexual harassment (e.g. Barak, 2005; Citron, 2009), and argued against punitive responses to girls and young women for digital abuse following the sharing of intimate material (Bailey & Hannah, 2011; Salter, Crofts, & Lee, 2013). Recent research also points to a need to map the ways in which different words travel and change meaning based on context and direction online (Kofoed & Ringrose, 2012).

Community and policy responses to cyberviolence against women and girls, however, have yet to be studied. Because of this, empirical research evaluating the success of prevention of cyberviolence against women and girls is virtually nonexistent. However, recent research more broadly on gendered and sexualized violence suggests that healthy relationship programming and bystander intervention models can help to reduce violence generally. For example, a majority (83%) of teens that participated in a violence prevention program indicated that they learned how to recognize an abusive relationship and know what to do if they or someone they know is being abused. In this same study, 3 out of 5 (60%) of students in a high school with a violence prevention program noticed a decrease in violence and bullying in their school and in the broader community (Canadian Women’s Foundation, 2011).

Recent research on media campaigns surrounding bystander intervention suggests that this is a promising approach for sexual violence prevention (Banyard, Moynihan, & Plante, 2007; Potter et al., 2009). One psychology study looking at cyber-bystanders found that people were less likely to intervene in online spaces that they perceived as highly monitored and under surveillance (Palasinski, 2012). This simulation suggests that further research is needed surrounding the conditions under which people are likely to act to prevent online abuse.

In terms of prevention strategies specifically for cyberviolence, the exploratory report Sexual Violence and Social Media: Building a Framework for Prevention (Fairbairn, Bivens, & Dawson, 2013) included 12 key recommendations. Selected recommendations that may be particularly relevant for OCTEVAW’s project are:

- Explore how social media and sexual violence intersect with other issues (e.g. mental health, racism, alcohol use);
- Focus on ground-up approaches that engage youth in all aspects of prevention programming;
- Promote healthy relationships and sex education, emphasizing conversations about consent, coercion, intimidation, boundaries, and respect.
- Foster knowledge sharing and collaboration among those working to prevent technology related harassment and abuse and sexual violence prevention.
- Partner with schools. Identify ways to integrate sexual violence prevention into curriculum activities and to engage youth leaders and community role models, while remembering that not all youth can be reached through school systems.
• Pursue critical media skills and bystander intervention. Engage youth as teachers of social media as part of developing critical media skills. Provide opportunities and resources to educators and frontline workers for social media training and programming.

Additional research themes indicate that cyberviolence needs to receive increased recognition, and that educational campaigns are likely to be more effective than harsh sanctions for abusive behaviour online (Bossler, Holt, & May, 2012). Despite this acknowledgement, to date there has been a lot of focus on educating young people about the risks of information sharing as increasing their risk of victimization (Ybarra et al., 2007; Bossler, Holt, & May, 2012).

One idea that is not included in these recommendations is to engage social media companies. While academic research does not seem to have explored this area as of yet, advocacy work discussed earlier point to this as an important strategy. Specifically, the research and advocacy undertaken by organizations such as the Association for Progressive Communications/Take Back the Tech has clearly been successful in raising awareness about cyberviolence more broadly and in analyzing social media sites responses to such violence.

**Implication for OCTEVAW:** During strategy development consider working with the PSYAC to develop a creative digital piece (‘Zine, spoken word, video, blog, etc.) about how they view safety online. Think about flipping the narrative of “how youth can stay safe online” to “how to help youth create safer spaces/better experiences online”. Consult with In Love and In Danger to explore potential overlaps/collaboration.

Finally, one area where research offers further potentially relevant innovation is in developing quantitative measurement strategies for cyberviolence. Ritter (2014) notes that although much research has been done regarding face-to-face sexual violence, and much theoretical work has been published regarding the nature of digital technologies, there is currently no scale created to empirically examine online sexual harassment (Ritter, 2014). Although Ritter’s research was conducted in the context of studying workplace-related online sexual harassment, this study presents an interesting framework for thinking about preventing cyberviolence against women and girls more broadly. (Additionally, the participants are undergraduate and graduate students with a mean age of 22, which is within OCTEVAW’s target age group.) By creating scales for online harassment and measuring these in relation to individual perceptions of online environments, Ritter found that perceptions of the online environment as stimulating (where risk taking is exhilarating), and as an environment in which blatant prejudice is acceptable, to be related to multiple forms of cybersexual harassment.

The implications of the above inquiry point to a need to work from a place where online spaces are approached as environments that can influence (encourage or discourage) cyberviolence. Additionally, it may be of interest to work with youth to create a scale or checklist of behaviours that constitute cyberviolence, developing this from the working definition to be created.

**Best practice:** Building on the definition of cyberviolence, consider working with youth to create a depiction (e.g. scale/image/checklist) of cyberviolence behaviours.
Part 4: Let’s Tech About It: Social Media Governance

This section looks at emerging work on social media site governance. Specifically, it explores (1) findings on the impact of social media structures on girls’ and young women’s experiences online (2) what we know about the nature of social media structures and policies to address cyberviolence, including social media companies’ responses to cyberviolence to date.

Impact of social media structures

Recent research conducted in Ontario can tell us a few things about the impact of social media on girls’ and young women’s experiences online. The eGirls Project\(^\text{16}\) interviewed six girls aged 15-17 and six young women aged 18-22. An additional 22 girls and young women participated in focus group discussions. Regarding the types of abuse experienced, Bailey (forthcoming) explains:

Canadian federal policy debates related to children and technology tended to focus on sexualized dangers posed by unknown adults. In contrast, many of our participants were clear that being online wasn’t “all bad”. When they did discuss online fears and dangers, their concerns tended to relate more to harassment and surveillance by known others (apart from stranger-related concerns they sometimes expressed about their younger sisters and girl cousins). This kind of gap seems to reflect a well-documented trend of policymaker focus on sexual threats from unknown predators, despite clear evidence that girls and women are most a risk of violence by those known to them.

This Ontario-based research with youth thus supports broader findings that we should be less worried about “stranger danger” when it comes to sexual violence and more focused on peer relations (recognizing that young people may be interacting online with peers/friends/followers that they know online, but not in the so-called real world).

Importantly, the eGirls project found that online architecture rewarding disclosure (e.g. through friend counts) while making it different to exercise privacy strategies, combined with personal choices, social norms, and gendered marketing practices, creates a “perfect storm” environment that facilitates conflict (Bailey, forthcoming). Additionally, having to disclose personal information with little understanding of what happens to that information, due to complicated privacy policies and terms of service, was identified as a problem. For example, Heath (forthcoming) explains:

Although girls and young women were portrayed in policy as being unaware, nor considering the consequences of their actions online, the participants clearly expressed

\(^\text{16}\) The eGirls Project is a 3-year research project that investigates the relationship between gender, privacy and equality in online social networking and is focused on better understanding the perspectives of girls and young women in relation to these issues. \(\text{http://egirlsproject.ca}\)
discomfort regarding the need to share (so much of) their personal information and were concerned with what corporations sought to do with that information.

Consequently:

We need to make available safer ways to participate in SNS, which do not threaten the security of one’s personal information. For example, more control over one’s privacy settings in a clear and understandable manner appears to be one way to improve the experiences of girls and young women online (Heath, forthcoming).

Overall, this report points to gaps between girls’ and young women’s’ understandings of their experiences online and those of policy makers (Bailey, forthcoming). Youth participants put forward the following recommendations:

• Bring online platform providers under greater scrutiny and directly target underlying systemically discriminatory social and marketing norms and practices that they understood to heavily influence girls’ ability to freely navigate their seamlessly integrated online/offline world.

• Approach surveillance as a problem, not a solution.

• Regulate platform providers to improve our privacy in simple, easy to understand ways.

• Require platform providers to make it easier to remove “cyberbullying”:
  o Clearer language on social networking sites about what “cyberbullying” is
  o Quick responses to “deal with the situation right away”.

• Provide support for targets of “cyberbullying”.

• Address problematic underlying social norms, not just the symptoms.

Privacy, defined as the ability for girls and young women to understand and control who has access to their data online, is an important piece of this broader picture of safety and well being.

Steeves (forthcoming) explains that

Although social media do provide girls with easy access to a wide range of popular culture products, they also provide commercial producers and marketers with easy access to the girls themselves…Requiring corporations to provide girls with better technical tools that allow them to control the lines between their multiple audiences will help them better manage the fluid movement of cultural capital between the private sphere of creativity and identity play and the public sphere of performativity and resistance. Restricting native advertising and behavioural targeting on social media will help insulate girls from the negative affects of media stereotyping and push back against commercial surveillance. But perhaps most importantly, we need to create non-commercial social-
technical spaces where girls can express themselves and project resistive identities into the public sphere.

**Best Practice:** Advocate for social media companies to produce straightforward, easy to understand privacy policies, and/or consider ways that these could be translated by youth, for youth.

Additional findings from the eGirls’ study suggest that participants perceived differences based on gender, race and membership in the LGBTQ community (Bailey, forthcoming) that girls living in urban settings may be “more likely to respond to an intervention that unpacks the online power dynamic involved in cyberbullying” (Burkell & Saginur, forthcoming). For OCTEVAW’s project, this further supports the idea of taking an intersectional (Crenshaw, 1991) approach to programming activities that centers the experiences of historically marginalized groups, such as holding workshop specifically to focus on the experiences of LGBTQ youth, and young women of colour, with cyberviolence.

**Best Practice:** Create programming spaces to specifically focus on the experiences of historically marginalized groups such as LGBTQ youth, and young women of colour, with cyberviolence.

### Social media policies to address cyberviolence

In the past year we have started to see advocates and activists focus on social media governance (site structure and policies) as an important area of intervention in cyberviolence. Emerging work by the Association for Progressive Communications (APC) (Athar, 2015) explores the nature of social media policies to address cyberviolence. From April 2013 and June 2014, APC and partners from seven countries\(^\text{17}\) conducted research looking at:

> The availability and effectiveness of corporate policies in facilitating women’s and girls’ access to justice when they experience gender-based violence - including sexual harassment, sexualised abuse, stalking, threats, coercion, blackmail and/or extortion – through the use of ICT [information communications technology services]” (p. 5).

The final report, released in March 2015, explores cyberviolence including:

- “Creation of “imposter” profiles of women, often to discredit, defame and damage their reputations.
- Spreading private and/or sexually explicit photos/videos, often with intent to harm, and accompanied by blackmail.
- Pages, comments or posts targeting women with gender-based hate (including misogynistic slurs, death threats, threats of sexual violence, etc.).

---

\(^\text{17}\) These countries included Bosnia and Herzegovina, Colombia, Democratic Republic of Congo, Kenya, Mexico, Pakistan, and the Philippines.
• Publishing personal identifying information about women including names, addresses, phone numbers and email addresses without their consent.” (p. 20)

APC notes that “Most of the larger web-based social media and networking platforms (Facebook, Twitter, Google+, WordPress and other blog-hosting sites, YouTube, etc.) now have tools to increase individual safety and security online” (p. 40). The following summary of options currently available to individuals is directly from APC’s report (Athar, 2014, p. 40).

**Tools to increase individual safety and security online:**

• Report inappropriate and/or abusive content (photographs, videos, comments, blog posts, pages)
• Report and/or block an abusive user from contacting you
• Report privacy violations, including fake profiles and the publishing of private or identifying information.

**Generally, “Report” buttons and forms can be found:**

• Located next to each function (such as the comment section, underneath photos, or message inboxes)
• In a navigation menu or sidebar
• In various “Safety”, “Security”, “Privacy”, “Community Standards”, or “Policy” centres/pages/settings. Users should keep in mind that each platform is different and often, reporting mechanisms are not centralised.

**When filing a complaint or reporting content, APC recommends that:**

• Users should keep detailed records (e.g. photographs, screenshots, emails, recordings of conversations) of all communications with the company – including the time, date and wording of reports, responses and decisions. Individuals’ records can then be used to hold companies accountable for their decisions on reports and complaints.
• Companies may not list all of their legal obligations or reporting mechanisms and procedures online; therefore users may need to telephone headquarters and hotlines to request all pertinent information for recourse. Individuals may need to file official requests with a company’s legal department.
• For threats to physical safety, police and investigative services are the first point of entry. Court orders, police warrants, or directives from cyber crime units are typical steps taken before companies divulge identifying information on abusive users to law enforcement. These must be availed of through formal legal reporting mechanisms.
• Emergency disclosure mechanisms may exist for companies to expedite cooperation with law enforcement, and law enforcement can contact companies through official channels in this regard. However, international cooperation with law enforcement depends on whether bilateral or multilateral treaties between countries exist.
• The terms of service generally detail which national laws and jurisdiction the sales contract is bound by, and therefore under which jurisdiction formal complaints will be processed and handled.
Larger national and international companies tend to have specific point people to address trafficking and child exploitation, which is useful in cases of violence against girls who are under 18 years old.

*Local ICT industry regulatory authorities may present an alternative forum for complaints* if users feel a company is in breach of its responsibilities and obligations towards consumers.

Most relevant for the social media policy aspect of OCTEVAW’s project, APC’s work reviews the corporate policies (terms of service and privacy policies) of the various “Internet intermediaries” who were implicated in their 24 cases studies of women’s and girls’ experiences of cyberviolence, as well as “those with a large share of the national market” (p. 7). This resulted in reviewing the policies of 22 companies in total. These include social media and networking platforms (e.g. Facebook, Twitter); telephone and Internet providers in the countries analyzed; search engines and portals (e.g. Google), and pornography websites (e.g. YouPorn).

This study also sought interviews with public policy representatives of the same Internet intermediaries, to (a) gain insight into the effectiveness of their implementation of policies and redress mechanisms in responding to VAW, and (b) document creative initiatives that companies have undertaken to promote awareness on gender, sexuality, VAW and human rights (p. 7). Significantly, this report notes, “Despite research teams’ repeated attempts to contact companies, most companies were not willing to participate in the research or discuss the topic publicly” (p. 7). Of the 22 companies, approached, only 6 were willing to participate in interviews.

To remain relevant to OCTEVAW’s project, this report will focus on the results of the social media and networking platforms, and search engines and portals. APC reviewed the policies of six social media and networking companies: Facebook, Google+, Instagram, Twitter, WordPress, and YouTube. A major challenge identified in social media policies is the lack of information about abuse reporting processes. As Athar (2015, p. 20) explains:

> Interestingly, most of the companies reviewed do have mechanisms in place that should technically respond to the above violations. However, it is impossible to assess the effectiveness of these mechanisms due to the fact that little to no public information is available about how internal review processes work. This includes how complaints are dealt with, what the ratio of complaint handlers to the volume of complaints is, what kinds of training on gender, sexuality, law and human rights the staff receives, the time limits for the review process, and clear policies on whether complaints are brought to law enforcement and under what circumstances (p. 20).

APC’s research explores the policies of Facebook, Twitter and YouTube, analysing the steps the companies have taken in response to controversial content. To address cyberviolence, APC puts forward nine key recommendations for social media governance:
1. **Recognize the importance of social context in formulating content-regulation and privacy policies, particularly in regards to VAW.**

This includes differentiating nudity from “obscenity”, sexually explicit content, and/or pornography. As Athar (2014) explains, Facebook has been the target of social pressure from women to change its policy to take social context into account and separate nudity (e.g. breastfeeding photos) from pornography. Facebook’s policy now states:

> Facebook has a strict policy against the sharing of pornographic content and any explicit sexual content where a minor is involved. We also impose limitations on the display of nudity. We aspire to respect people’s right to share content of personal importance, whether those are photos of a sculpture like Michelangelo’s David or family photos of a child breastfeeding.

Community responses such as the Women, Action, and the Media (WAM!) Facebook campaign noted earlier pushed Facebook to ban pages that glorify gender-based violence and hate, rather than categorizing it as humour. Specifically, between 2012 and 2013, Facebook and Twitter both came under intense public pressure for failing to take any action on content that promoted, glorified, or threatened women directly with rape, sexual assault and physical violence (Athar, 2015). Yet,

> It was only after large public campaigns condemning the companies’ inaction, and advertisers threatening to drop their spots, that they took any public stance on the issue. Facebook issued a single apology and statement that it would update its training to address gender-based hate, and Twitter brought in new reporting and blocking mechanisms for its users. While these are positive steps, it remains to be seen how effective these changes will be, especially without any transparency on what trainings on gender, VAW, laws and human rights are being provided to content-reviewers at these companies.

APC finds that YouTube’s policies provide users with perhaps the most concrete definition of unacceptable portrayals of violence and inappropriate content. Their policy states: “It’s not okay to post violent or gory content that’s primarily intended to be shocking, sensational or disrespectful,” and states that “if your video asks others to commit an act of violence or threatens people with serious acts of violence, it will be removed from the site.”

2. **Strictly prohibit the publishing of private, confidential, and/or identifying information of others.**

Along these lines, APC identifies a need to clearly define “private” and “public” information. They found it is unclear what constitutes “publicly available information” on social media sites. They argue that:

> Companies genuinely concerned with privacy should make user profiles completely “private” as the default setting, encouraging users to make informed and individual
decisions about what information they choose to share and make public. Yet the trend is the opposite, and increasing personal data in the public realm can present heightened safety risks for individuals. (p. 23-24)

3. *Address the English language bias in reporting mechanisms.*

APC finds it is unclear whether the abuse reporting forms are available across languages, and that it is unknown to what extent the staffs responsible for processing takedown requests are multilingual.

**Best Practice:** Organizations should explore to what extent language barriers may be an obstacle for youth accessing supports/reporting abuse online.

4. *Promote mutual legal assistance treaty (MLAT) reform to increase access to justice in cases of technology-related VAW.*

APC explains that mutual legal assistance treaties (MLATs) are the primary means through which US-based companies cooperate with law enforcement in other countries, particularly around criminal investigations. APC argues that companies should provide greater transparency in this regard. While this is an important legal action worldwide, it is likely not a focus of OCTEVAW’s project.

5. *Provide greater transparency and accountability regarding (in)action on content and privacy requests; and*

6. *Provide greater transparency and public accountability about the departments and staff responsible for responding to content and privacy complaints.*

In APC’s multiple case studies, women reported either a total lack of response, or an automated response from companies that did not include detailed information: e.g. a timeline for action, what action (if any) was taken, and why (or why not) content was removed (Athar, 2015).

Additionally, there is little to no information available publicly about (a) the number of staff/teams dealing with complaints, (b) the languages they speak, (c) what training is provided on gender, sexuality, VAW, law and human rights, or (d) where the teams are located. Facebook presents a positive example by providing an infographic and a webpage explaining “What Happens When You Report even this still stops short of providing exact details (p. 26).
This recommendation fits with Ontario findings on girls’ and young women’s experiences online. One possibility for youth engagement here would be to ask youth project volunteers to report incidents of cyberviolence and to track this process. This fits well with one of APC’s identified area where more knowledge is needed. Specifically they identify a need for work that:

systematically documents (a) women's/girls' attempts to report content and privacy violations to specific companies, (b) the responses they received, and (c) the timeline of (in)action. Building this evidence base will highlight where where key gaps in women’s access to justice lie, and provide a valuable resource for those concerned with laws and policy formation around VAW, business and human rights (Athar, 2014, p. 42).

One platform that the APC did commend was Google, which they describe as having
a particularly elaborate transparency portal, where it details content-takedown requests by “reason”, including categories for “impersonation”, “hate speech”, “violence”, and “bullying/harassment”. Google’s model\(^\text{18}\) is a small step towards providing greater information on responses to technology-related VAW, and could be expanded upon and incorporated by other companies’ reporting systems as well (p. 37).

**Implication for OCTEVAW:** During strategy development consider asking youth project volunteers or the PSYAC to report incidents of cyberviolence and to track this process. This information could be provided to social media companies to illustrate gaps and/or discrepancies between how their policies say they will handle cyberviolence and what actually happens.

7. Reserve the right to terminate accounts specifically on the basis of repeated gender-based harassment, hate and abuse; and

8. Ensure system-wide removal of individual content (photos, videos, tweets) at source.

Social media and networking platforms often have a standard disclaimer allowing them to terminate a user account if the account violates any of the terms of service\(^\text{19}\) (Athar, 2014). Yet APC finds that “as with other intermediaries, protecting intellectual property rights appears to be the main priority for social media companies” (Athar, 2014, p. 27). Facebook and YouTube are the focus here, where account suspensions are “only mentioned as a consequence in relation to copyright infringement” and YouTube’s Account Termination policy “lacks a clear stance on hate, abuse, violence and privacy violations” (Athar, 2014, p. 27). APC argues that

---

\(^{18}\) google.com/transparencyreport/removals/government

\(^{19}\) Athar (2014, p. 9) explains that: “Terms of service (ToS) are legal contracts between companies and their users, outlining the responsibilities of each party. ToS primarily serve to protect corporations from any legal liability and damages resulting from the use of their services and their operating procedures; yet these policies also demonstrate what a company views as (un)acceptable behaviour and a breach of terms. No matter how limited, the ToS and their processes may serve as a space within which individuals can access certain remedies. Individuals concerned with privacy and security should be aware of the ToS of any platform.”
Multiple strike policies should be expanded beyond copyright concerns and implemented for accounts that repeatedly infringe others' rights to privacy, security and bodily autonomy more broadly: whether they repeatedly harass, intimidate and/or abuse others, repeatedly create pages that get flagged and removed, or repeatedly post private information (including photos, videos or identifying information). (p. 29)

Regarding point eight, as APC explains, metadata refers to “technical details that help describe how, when and by whom a piece of user content was uploaded and how that content is formatted” (Athar, 2014, p. 29). All companies collect the metadata surrounding each piece of uploaded content, and APC explains that metadata should enable companies to track and trace content and its spread across their entire platform. Therefore, when non-consensual intimate photos and videos are uploaded and spread virally, metadata should therefore enable social media sites to takedown across an entire platform. APC states that, “While YouTube has a system to remove a video at its source, it is unclear whether the same mechanism is in place on Facebook, Twitter or Instagram” (p. 29).

In this regard, APC argues that:

Companies should show greater transparency in this regard, and move towards a clear system that enables this platform-wide removal system, including posts that have been shared, re-posted, re-tweeted, etc. by other users (p. 29).

In terms of pursuing the policy changes listed in points seven and eight, OCTEVAW may be most effective in this capacity by reaching out to other organizations that are already doing this work, for example, Women, Action and the Media and the organizations on Facebook’s Safety Advisory Board (discussed below).

9. Engage with experts in gender, sexuality and human rights to provide input into policy formation, staff training, and the development of education/prevention programmes.

In this final recommendation, APC explains that:

Facebook provides another positive example through its Safety Advisory Board, comprised of five prominent Internet safety organisations. In collaboration with the US National Network to End Domestic Violence, Facebook released “Safety and Privacy: A Guide for Survivors of Domestic Abuse” in July 2013. Facebook also has a Network of Support comprising five US-based LGBT advocacy organisations, and has commissioned research for its “Compassion Project”, which looks into bullying and harassment online. Such moves demonstrate a willingness and effort to learn from civil society on how to address rights issues. However, this engagement should be expanded to groups outside of North America and the European Union to better address the needs of users in other regions who actually make up the majority of Facebook users. Guides and research should also be made available in multiple languages to benefit the widest possible number of non-English-speaking users (pp. 29-30).
According to Facebook, the *Facebook Safety Advisory Board*\(^{20}\) “is comprised of five leading Internet safety organizations from North America and Europe. Facebook consults with these organizations on issues related to online safety.” These organizations are:

**Childnet International**
Childnet International is a UK-based charity working domestically and internationally to help make the Internet a great and safe place for children and young people, enabling them to use interactive technologies safely and responsibly. Childnet has developed a number of resources designed to help young people and parents assess and manage the risks they may encounter online. Visit Childnet International at [http://www.childnet.com](http://www.childnet.com).

**NNEDV**
The Safety Net Technology Project of the U.S. National Network to End Domestic Violence is the leader in online safety for survivors of domestic violence, dating abuse, cyber-stalking and harassment. Based in Washington, D.C., it represents coalitions against domestic violence in every U.S. state and territory and works to address technology and safety with sister organizations worldwide.

**Connect Safely**
ConnectSafely.org is the leading interactive resource on the Web for parents, teens, educators and everyone engaged and interested in youth safety on the Web. Visit Connect Safely at [http://www.connectsafely.org](http://www.connectsafely.org).

**The Family Online Safety Institute (FOSI)**
The Family Online Safety Institute works to make the online world safer for kids and their families by identifying and promoting best practice, tools and methods in the field of online safety that also respect free expression. Visit FOSI at [http://fosi.org](http://fosi.org).

**WiredSafety**
WiredSafety is the largest online safety, education, and help group program in the world and provides help, information and education to Internet and mobile device users of all ages, especially on cyberbullying matters. Visit WiredSafety at [http://www.wiredsafety.org](http://www.wiredsafety.org) and [http://stopcyberbullying.org/](http://stopcyberbullying.org/).

Even without a social media site directly involved in the project, OCTEVAW and/or one of its project partners (e.g. Media Smarts) could reach out to these organizations to see if there might be opportunities for collaboration and mutual support.

Some additional strategies for advocates to engage social media companies on cyberviolence that APC identifies (Athar, 2014, pp. 41-42) are:

- Organize media campaigns to raise awareness on technology-related VAW, calling on companies to:
  - Cooperate formally with anti-VAW groups and women’s rights groups to input into policy formation and planning.

\(^{20}\) [https://www.facebook.com/help/222332597793306](https://www.facebook.com/help/222332597793306)
o Fund research, education and prevention initiatives on issues of bullying and harassment, especially from a gendered-perspective.

o Create legal information centres that detail the laws and liability measures that a company is governed by, including any voluntary initiatives from pertinent ministries.

o Build upon transparency reports and formal annual reports to include specific details of how the company has addressed VAW, as well as other human rights abuses.

- Lobby industry leaders and other companies to use their business relationships to pressure ICT platforms and services to take a formal stand against VAW.

- Input into the drafting of new or amended legislation surrounding issues of technology-related VAW, including reviews of liability and systems of judicial oversight for companies on this topic.

- Support ICT platforms and services that demonstrate a commitment to anti-VAW work and human rights, which can encourage greater competition and reflexivity within the industry.

This critical work by APC highlights a need for further work that attempts to engage social media governance as an area of change. Specifically, both eGirls research participants and APC research identify clear, simple privacy settings and transparent reporting processes as necessary for preventing cyberviolence and enhancing girls’ and women’s well being online.

Additionally, APC research suggests that although social media companies are taking action to prevent cyberviolence through some existing partnerships, it is very difficult to get social media companies directly engaged in this area, but that they respond well to public pressure from coalitions and collective efforts. As such, reaching out to those who are connected to social media companies is likely to be a more effective strategy than trying to get a social media company directly involved in OCTEVAW’s project.

**Implication for OCTEVAW:** Take needs assessment findings back to youth involved in the project and the PSYAC, and find out what interventions regarding social media governance are of most interest and importance to them. Develop a small number (2-3) of specific, concrete changes that they would like to work towards/advocate for, and develop a timeline of action.
Conclusion

This needs assessment report has outlined what we know about cyberviolence by breaking it down into three central components: online harassment, non-consensual distribution of intimate images, and cyberstalking/digital dating violence. It has explored academic literature and news coverage, highlighting specific themes of this coverage as well as social media sites and/or apps that are the focus of coverage. Additionally, it has discussed emerging themes highlighted by several high profile media cases that have contributed to broader social awareness of cyberviolence against women and girls. Finally, it has also overviewed social responses to cyberviolence to date and emerging work on social media site governance, emerging issues and themes young women are experiencing, as well as youth-led strategies and responses to further develop throughout this process.

Feasibility of a code of conduct model

OCTEVAW has explored the feasibility of developing a “code of conduct” model (voluntary code for social media companies to adopt that promotes empowering spaces for girls and young women and prevents and eliminates cyberviolence) with the aim of preventing cyberviolence against women and girls. While the project coordinator in consultation with the Youth Advisory Committee should ultimately make this decision, a few points on feasibility can be drawn from this inquiry and recommendations:

1) Much work to date in the broader cyberbullying literature has focused on individual-level strategies to create safer online environments. If working to develop a code of conduct, it would be most useful to focus on peer group, community, social, and structural practices (e.g. social norms, site governance) as much as possible to expand/bridge out from the focus on individual behaviour.

2) A ‘declarative’ approach identifying cyberviolence as an area of importance, with guidelines for prevention/bystander intervention, may be more feasible than a prescriptive behavioural approach. In other words, it may be more realistic to come to agreement about the nature and severity of cyberviolence, and affirm a commitment to preventing this violence, rather than to come to consensus about specific online conduct. Examples of declarative campaigns/documents might include the Declaration on the Elimination of Violence Against Women and/or the White Ribbon Campaign.

3) The Ontario government has recently released a powerful new PSA “#WhoWillYouHelp” featuring (among other scenarios) a bystander intervention in non-consensual sharing of intimate images. Additionally, OCTEVAW’s “I Can MANifest Change” campaign has been a successful model of PSA’s and individual pledges to by men to prevent violence against women. Building on this work and momentum, engaging Ottawa community members to make a commitment to ending cyberviolence in various ways is a seemingly rich and feasible area of work.
4) There are several high-profile organizations (e.g. Women, Action, & the Media [WAM]) currently working in partnership with social media sites to address abuse and harassment occurring on their sites. Given this, partnering with high profile sites such as Facebook and Twitter to encourage them to adopt a code of conduct seems unlikely. However, those stakeholders currently entering partnerships such as WAM may find such resources useful to inform their work, and more locally-connected social media-tech folks would likely benefit from such an approach.

What Young Women Want: Emerging Themes

Throughout this needs assessment process we spoke to young women across Ottawa in high schools and university, as well as engaged with the Purple Sisters Youth Advisory committee, as it is important to listen to youth directly. From these discussions we were able to highlight emerging themes in cyberviolence through young women’s perspectives. The engagement and discussions with young women and girls witnessed throughout this project particularly focused on the different themes to address issues such as governance, privacy, consent, and the gendered impacts of “cyberbullying”, in order to adopt approaches and strategies that reflect young women and girls experiences in their daily lives and communities. During the needs assessment process we asked both about young women and girl’s experiences with sexual violence and online social media and about the issues and responses identified within technology platforms. In this section, we focus on the key themes and issues identified by young women and girls for young women and girls throughout Ottawa. Many of these themes and issues echoed many of the great studies highlighted in previous sections of this report, such as the eGirls Project and Young Women in a Wired World, it will be noted when these studies resonate with the young women we spoke to.

Note: all youth participants consented to audio & note recordings but collectively decided that any direct quotes used were to be attributed simply to ‘member(s) of the Purple Sisters Youth Advisory Committee,’ ‘youth engagement leader,’ ‘participant’, or just ‘the PSYAC’.

What does it mean to be a girl online?

Our participants were pretty interested in talking about all the different ways girls are being themselves online as well as all the pressures they are facing. Many of the young women we spoke to didn’t really know what it really meant to be a girl online except that it’s both an “adventure and a struggle”. This theme particularly corresponds with research from the eGirls project. Some participants talked about how hard it is to express yourself meaningfully, and some of them talked about how others spend way too much time seeking attention or posting inappropriate representations online. Like the eGirls project, most of the young women we spoke to weren’t interested in engaging in victim blaming other young women for their actions and experiences online. Instead, they situated their experiences within a larger system of constraints in the context of online engagement and self-empowerment, they practiced empathy and wanted to do pull apart the impacts of myths & stereotypes of normalized female beauty standards, and how these interacted within online structures and platforms.
“Cyberbullying” is overused and erases sexism, homophobia & transphobia

While some of the participants did not necessarily think that sexism informed “cyberbullying” many perceived clear gendered differences in the frequency and nature of “cyberbullying”. (Girls were being targeted more than boys online, trans feminine people especially, and the boys who were being targeted were being targeted because of their ‘feminine’ behaviours. This theme was also identified within the literature and particularly with the eGirls Project.

Overall, most of our participants feel that the term cyberbullying and its framework has lost all meaning because of its vagueness and the fact that it’s overused. Young women want us to know that cyberbullying is not taken seriously. They deeply feel that it is treated on the same level of teasing, when in fact what young women are really experiencing is perpetual and sustained attacks of violence because of their gender. Young women want us to use the term cyberviolence or cyberharassment and feel that it’s integral in order to not undermine what is really going on, which is linked to the hatred of femininity, sexism and homophobia and transphobia. One of the PSYAC, age 17, had this to say:

Words like cyberbullying are overused and are pretty a playful menace. Everyone always hears about cyberbullying but nobody takes it seriously. It’s pretty much on the same playing field as teasing and we downplay it. When anyone comes in to talk to us about cyberbullying nobody listens. We don’t listen because it doesn’t mean anything to us and most of the time they are trying to scare us to not sext anyway. Seems pointless.

Fear is not the best strategy

Young women & girls want us to know that the Internet is not exactly the dangerous and evil place adults make it out to be, but that it has the potential to be a crucial space where their lives, communities and experiences grow and thrive. Young women want us to know that preventing cyber and sexual violence should not focus solely on the negative side of online life and that hey, young girls are going to be online regardless. Instead of telling young women to fear online give them the information they need to make the best choices for them. Most young women emphasize the social, community, & entertainment aspects of keeping in touch online which is also another emerging theme noted in the eGirls data.

Don’t do this, don’t do that

The PSYAC & other young women expressed that their school-based education around media literacy was predominately framed in terms of how they should not steal music or post inappropriate photos, how they should not access certain sites on school computers or at home, and most importantly how someone is always watching and waiting to catch them if they do something wrong online. This intertwined with subtle references to “the government,” “the police,” “the principal”, “school social workers”, “parents”, “a predator” and other actors routinely named by participants as potential surveyors monitoring their online presence. As these statements suggest, any formal education is focused largely on “safety planning” and policing their interactions with social media, typically motivated by fear and myths surrounding the
Internet. What young women did tell us was that any education they’ve received on media literacy or cyberbullying has yet to provide any truly meaningful strategies to negotiate social networks in an informed way, let alone design one that would capture the complexities of experiences. As the eGirls data suggests, young women want adults to stop sending them mixed messages about what it means to be online, and to let them make choices for themselves while providing access to the best and most useful information.

Young women want to know more

Many of the young women and participants explicitly cited an interest to ‘know how the Internet worked’ or to ‘learn how to make media online’. Almost all of the participants wanted to explore what it meant to be a young women online & what does preventing cyberviolence look like, as their motivation for participating in the project. As one stated, “I always wanted to work with the Internet but not, like, entertainment stuff. I want to be able to be part of the change because we all know how friggen’ hard it is to be a girl, even online.” In most cases, they specifically mentioned how unhelpful they’ve found their formal education to be in addressing the issue of cyber and sexual violence and it’s relation to being a young woman or girl.

Loss of control

Participants as well as the PSYAC felt more experienced than their parents or teachers in how to be online & the realities of using technology (both the positive and negative experiences). The PSYAC had fun browsing photos of themselves, friends, and even strangers on Facebook and Instagram. They also expressed concern that someone “creepy” could be looking at their photos or the photos of friends and family members. Concerns were also raised that they could lose control of their online representations by losing control of what photos of themselves get posted where and when. PSYAC members often instructed each other of the consequences of posting of a photo of oneself to Facebook or other social media could come back to haunt them later in life if found by a college or employer. This constant fear of shame and permanent damage was a recurring theme throughout the workshops and focus groups. When young women discuss issues of online fears or dangers, they focused heavily on the potential to make one mistake that could cause permanent damage to their reputation, career, education and social lives. These fears frequently revolved around the issue of sexualized self-representations or representations that they have little control over online (Bailey & Steeves, 2014).

Not just about risk

Although these concerns were felt and often noted, some PSYAC members would still take photos of themselves or others and post them online. Even the participants who often lectured others about uploading certain photos would themselves participate in this practice, especially with selfies. The PSYAC were experienced in the nuanced and often contradictory emotions and practices that come with being young women and engaging online and what the gendered impacts are. They understood wanting to interact with their peers while simultaneously wanting personal privacy and tight control over their own experiences and representations. Holding on to
these often contradictory and messy tensions provided our young women with a common experience that they felt were not necessarily shared with adults. It was frequently noted that parents, teachers, mentors, grandparents, or other adults seemed to lack a ‘common sense’ that they and their peers share. This is not to suggest that these adults don’t know the Internet, but that young women alike often felt adults were less experienced and thus didn’t quite understand how complicated it all really is online.

**Give us some credit**

Many of the participants described themselves as more capable of negotiating their privacy, property, and security than their teachers, mentors and especially their parents. Disclosures of managing a parent’s engagements with the Internet to ensure a certain degree of personal privacy were most common, as in this example from a 15 year old participant:

> Well, like my mom is kind of annoying how she like— like she's a great person, but how sometimes when she gets on Facebook, she'll just start clicking. So, if she sees anything that I've been tagged in, she'll click on it and go through the whole album and comment everywhere

Not wanting her mother to see every photo that gets posted to Facebook, but also not wanting to hurt her mother’s feelings by “defriending” her, this young person configured her mother’s Facebook privacy settings to enhance their own privacy:

> So, what I did was I went on her—when she went to the bathroom and she was on Facebook and I went on there and I went into my profile and I said ‘hide all posts.’ So, I don't think she can see it, but I asked her ‘would you be mad if I defriended you’ and she’d be like ‘yeah!’ But it's so obvious if you block someone, it's even just like defriending them. So really, you can’t really block or defriend someone who’s still like in your group or family .. so you have to get creative and know all the little details of how Facebook works.

**Blocking our social media**

The PSYAC frequently discussed experiences with their schools blocking access to Facebook, Google Chat, Twitter, and other “non-educational” or “fun” media from school computers. That school filters were discussed as easy to bypass on school computers with proxy sites such as HideMyAss.com, or simply with a smartphone to access the Internet while at school, indicates they do little to deter access to such media for young people intent on accessing them yet don’t acknowledge responsibility. What was communicated by these filters, and expressed by young women, was a felt presence of institutional surveillance and censorship that framed certain media as ‘unproductive’ in and irrelevant to their formal education when a lot of young women felt that it was important in their social and emotional lives and well-being.

Such framing also harm the ways young women share personal knowledge through an accessible social network. Blocking social media such as Facebook, Twitter, or Google Chat on school computers hinders a student from accessing the classmate who can help them with a math problem, or the friend who provide them with emotional and social support to navigate a
complex and often violent world. Young women increasingly share and collectively produce support and knowledge in these ways and this could be an important mechanism for preventing cyber and sexual violence.

**It’s not just about stranger danger**

Many young women expressed as much or more concern about online surveillance by family members, employers and peers as surveillance by unknown adults. One young woman stated, “I was getting stalked by my boyfriend and had no one to talk to about it”. As discussed above, for many of our participants, peer surveillance and policing were integral components of cyber and sexual violence. Young women expressed experiencing violence and harassment from their family, partners and peers more than strangers online.

**Challenging sexism & rape culture online**

Young women advocate that addressing the issue of cyber and sexual violence in any meaningful way, as well as deconstructing the stigma and shame young women and girls are experiencing requires the development of better support networks, accountability frameworks and educational responses aimed at dismantling systemic oppression and violence. Young women and girls have explicitly stated that sexism, misogyny, homophobia, transphobia and racism are emerging issues that must be addressed through gender-based strategies.

“[…] Definitely, not only are they [young women] targeted more but often the language boys use to insult each other is sexist and/or misogynistic. So whether either gender is being targeted the underlying theme is usually misogyny. Girls are also more often the targets of online body shaming, body policing and slut shaming.” -Carleton University Student, Age 22.

**It’s not consent if we can’t understand**

When young women voiced their displeasure with the way Facebook frequently asked them to submit to a Terms of Service policy that they felt was too long to read and too complicated to understand, we asked ourselves what is the underlying issue in these young women’s experiences.

‘Why can’t Facebook do it like this?’ Was a common expression voiced by young women. Through critical examination of some policy and platform design, young women came to see governance policies as complex processes carried out by actual people rather than protocol inherent with the technology itself. This meant that the young women could imagine technology and platforms operating differently.

As we unpacked this further, property and profit emerged as key issues in our critical analysis. Young women ask “is personal information the participant’s property to disclose and control access to within a platform, or is it the platform’s -- and thus its proprietors’ -- property? These questions led to some important re-thinking regarding the Internet and cyberviolence. Young women identified that these platforms and technologies, and their proprietors (often for profit corporations) have an ethical responsibility to intervene in situations of cyberviolence on their
platforms. Young women also feel it’s important that others like them understand the context of engaging with these online proprietary technologies. Young women also feel that it’s the platforms responsibility to explicitly state their intentions and use of any content submitted to their platforms and who has the right and ownership over this content. In this way young women would have more sense of control and ownership and can make more informed choices online.

“There is not enough accessible information being given to young people about how the Internet works and the legal implications of posting things online, cyberviolence, etc. The very nature and culture of many online platforms directly discourages consent and privacy. The default setting is to have everything public, which folks might not realize. This leaves people open to stalking and potential sharing of information they believed was private.” –Young woman, 21

**Surveillance: there’s an app for that**

In interviews with young women there was a common view that someone was always watching them and others through the Internet in an unexplainable way. At times this was expressed as some “conspiracy” other people believed. Other times, this was discussed though specific examples of legislation and court cases that gave them a sense of the government’s potential ability to watch and intervene in their lives in both positive and negative ways.

“Everything can be seen by the government, police or these technology companies. There's no such thing as privacy anymore. They say you can—any time your phone is on, you can be followed. Like even the new FB messenger can record your voice or something. Like you can be being traced, your phone calls can be listened to and if police wanted to get your text messages, they could get your text messages. Private or not. This is scary. And like, what does that mean for our safety and for being able to get help?” –Young women, age 15.

“Like I just know it. And I know that someone could see everything you do in a computer. Like if you’re doing like credit card scams and stuff like that, they could trace it back to that computer. It’s not even just the bad stuff going on, it’s the good stuff too. They have access to all your information. I think there’s even apps you can download that will steal all your content and people can use it in really messed up ways. Like this one app I heard of you can download it to like, copy peoples numbers and override your block list. So even if you block someone and don’t want them to contact you, they still can. Why do these apps even exist?” –Young women, age 21.

**Censorship & monitoring: to flag or not to flag**

One of the PSYAC members was offended that their school tried to regulate their Internet access with a content filter. This young women was able to easily circumvent the filter, but took the protective gesture as a sign that their school “didn’t trust I could think for myself.” At the same time, this young person stressed that such a filter could block them from important and useful content such as sites or apps online that could be used for school projects or to communicate with class mates related to school work. The young women expressed that by inherently not trusting young people it creates this culture of mistrust and undervaluing of their knowledge and expertise which ultimately affects their self esteem and access to self empowerment.
Another youth women discussed her concerns with racism online and how they felt the Internet allowed people to harass and spread racist content online such as “the KKK or terrorist propaganda”.

This young women felt more online surveillance was necessary to identify and “unmask” people engaged in online hate. She also felt it was important to censor racist language online. To address this concern, we debated how we might distinguish between what was and was not considered racist content, and considered the problems of having a small group of people evaluate and censor a larger group of people’s communications. While some content may be obviously racist, sexist, homophobic, or just spam, we reasoned that it may not be so easy to decide what was and was not appropriate content.

We decided that it could be useful for platforms to implement a content ‘flagging’ system in their network. How it could work is that participants would be allowed to post whatever they wanted but small flag icons could be automatically added to it so others could flag the content if they personally felt it was inappropriate. Some platforms already engage in these types of mechanisms but not all of them. When someone flags a piece of content, the platform would be so notified so they could evaluate the content together and decide if it should remain or be deleted. If more than a few participants flagged the content before platforms were able to evaluate it, the content is temporarily removed from the site so that it could be evaluated. This allows platforms to monitor potential spam or inappropriate content that other participants were bothered by, and allows platforms to take into account the judgments and feelings of participants. This also can create a temporary system where content that participants find particularly offensive could be removed immediately through collective action until platforms have a chance to consider it and decide if it should be reinstated or not. Some young people even suggest that platforms form a committee or have an outside organization audit content reporting in order to ensure that biases and discrimination aren’t missed throughout the flagging process. This also would provide some transparency and accountability from platforms.

Location services: off

‘Checking in’ or ‘tagging’ oneself at a certain physical location, a common practice on Facebook, Twitter, and Foursquare, was particularly unappealing to the PSYAC. While this practice is often flagged as dangerous by parents and teachers because of the way it potentially lets strangers know where they are physically located in real-time, this was not why the PSYAC singled out this specific practice on social media platforms. Their reasoning was twofold: they personally found this practice to be an “annoying” way that people publicly flaunted certain offline behaviors, and they found that it could do more harm than good in regards to cyber stalking and online intimate partner violence.

Private messages aren’t that private

Young women identified private messaging and chat apps as problematic and also related this to a social media governance issue. Initially the PSYAC assumed we couldn’t see the private messages exchanged by users in online chat and messenger apps. It was then explained that it would be possible for network administrators to see and collect any private messages if they
chose to look at them. This revelation of what information network administrators and platforms have access to, thus led one young person to reflect on the role platforms’ employees might play in compromising their personal privacy and safety:

Like, I know [with] Facebook not one person can man it by themselves – maybe when it first began. So, if you're constantly hiring new workers, that means that what was once secure is no longer secure. Because now multiple people that weren't supposed to know what was in the message now knows what content it held. And once they're fired, they're angry and they share that. So it just keeps going on and on and then in chain emails -- now the whole world knows what that message said and they could use it ways that are dangerous and not safe. And nobody really knows this about these apps and chat applications. They don’t really disclose it either.

As this discussion of privacy, safety and security unfolded another PSYAC member explained how they choose not to use any of Facebook’s privacy controls -- because they didn’t trust the usefulness of such controls:

I don't use my privacy settings because even so, there's always a way around. I feel like there are hackers out there no matter what. [Privacy] doesn't exist. It's a façade. Like it's something that somebody -- like they want to say, okay, we did this and that to make sure your page is secure just so they couldn't be blamed if something like they were hacked or things like that. And like, every time the app updates or there’s a FB update your privacy settings are suddenly all different and changed back to the general settings and they don’t notify you. So it’s like every time the code and platform changes, your privacy and safety changes. It’s not fair and nobody really knows that they do this. So we’re like making choices about stuff that we aren’t even aware of. You think you’re doing it safe, and it turns out your not.

The realization that there were people and practices that could not be stopped through the standard privacy settings caused the PSYAC to more critically consider the work such settings do if they don’t fully protect their privacy and safety.

**If it’s doable, do it: Ethics & technology platforms**

Young women and other young people do not have access to all the technological aspects of the Internet so when they found out more about secure socket layers (SSL) connections it often became a topic of concern in workshops and focus groups. SSL is a protocol for transmitting private documents via the Internet. Most web browsers support SSL, and many websites use this encryption protocol but many sites also chose not to use this extra secure feature in the coding of their platforms. You will often see this protocol when you are prompted to enter credit card information and the browser will request to store a trusted security certificate.

Another protocol for transmitting data securely over the Internet is Secure HTTP (S-HTTP). Whereas SSL creates a secure connection between a client and a server, over which any amount of data can be sent securely, S-HTTP is designed to transmit individual messages securely. SSL and S-HTTP, therefore, can be seen as complementary rather than competing technologies. Both protocols were approved by the Internet Engineering Task Force (IETF) as a standard, yet throughout our engagement process we learnt that many social networking platforms do not
engage in these standards and protocols which could leave users information and private data vulnerable and at risk.

Suddenly, what sites young people used that did or did not offer them an SSL or “https” connection meant something and was now regularly mentioned and debated. It wasn’t too long ago when Facebook had yet to begin offering SSL connections for its users. Once young people found out about this option they wondered “Why don’t all sites and platforms do this?”

Contrary to popular myths and misconceptions about young people, it became apparent throughout this process that young women are concerned about their privacy and data. They are concerned and hesitant to release private information when corporations like Google and Facebook try to collect their information (so they can potentially profit from it at a future date), yet they are releasing this information regardless because they know it’s what they need to do if they want to continue to engage with their friends online. These young women are making choices within larger systems of constraint, and this was also a theme identified by the eGirls Project. However, young women let us know that they want platforms to make it clear to the participant when they were collecting this information and what they were collecting for what purposes. They want platforms to make it clear their intentions with users content and their information so that they could make more informed choices.

*We deserve more than safety*

One thing was clear in our needs assessment process: young women are tired of cyberbullying narratives and tips for online safety. Being taught how to stay safe or out of trouble online was now discussed as more than just an annoyance. Such education was considered an interruption from what they wanted to be learning and what they felt would be empowering to learn. Beyond the classroom discussions turned to the “tech geeks” and Tumblr fanatics in their schools who they felt held much power because they were able to technologically outsmart parents, teachers and administrators. These tech geeks, for example, were discussed as among the first to figure out a way around school filters and to share this knowledge with other students. Their knowledge of the Internet gave them a degree of control and empowerment within their schools and this kind of media literacy, they felt, was severely lacking from their education and schools.

*Controlling the field of misrepresentation*

Young women seem to have grown tired of seeing the same misrepresentation in every parental advisory, school presentation or anti-sexting ads.

This raised the notion that there was a commonality in how these narratives presented young people as helpless victims in a dangerous environment; a representation they found inconsistent with the ways they and their friends presented themselves online, and damaging to their self-determination and empowerment.
**Emerging Possibilities: Identifying Strategies**

Some of the last discussions young women from the PSYAC had together during the needs assessment process was the strategy development idea generating sessions that served as an open dialogue to talk about what direction we should head following the completion of the needs assessment process.

The PSYAC had given many ideas and insights throughout the nine knowledge-sharing workshops but their central ideas surrounded 3 key ideas: A Online Vlog/Video Series, an Open Source Social Network and/or an Online Toolkit that would serve as a hybrid between a code of conduct and resource kit for young people, especially young women. The PSYAC were very excited at the prospect of creating their own digital media, particularly videos and blogs. The ideas of these strategies came from our knowledge-building workshops, data collected from young women in high schools and universities across the city, as well as from the engagement and creativity of the PSYAC themselves.

**Strategy 1: Creative Responses (Online Vlog Series)**

*A vlog, or video blog, is an online video publishing platform.*

**Strategy Possibility**

One of the main strategies that developed from these workshops was the idea to produce of an Online Vlog Series that allowed the PSYAC to asynchronously interview various key informants and experts through a documentary and workshop type format, this would provide the perfect space to build knowledge, inform and engage users in building prevention. Members of the PSYAC frequently lamented how their only formal education around the Internet was organized around issues of cyberbullying, sexting and non-consensual distribution of photos. So as we began to focus our concerns and identify our aims for producing a strategy such as a vlog series, we developed ten key questions that we wanted to ask people who had certain kinds of knowledge that we didn’t have. It is our idea to recruit privacy lawyers, social media marketers, tech workers, Internet governance people, online game developers, academic technologists, digital activists, Internet researchers, and online publishers who might inform our questions. The young women wanted to talk to people with the kinds of knowledge they do not have access to, and whom they would rarely come across in their environment. We also believe that it would be great to do a second series of the same format with other young folks and peers and develop a separate set of questions.

Here is a draft of some questions we have generated for the possible Vlog Series:

1. What is your job and how does it connect to the social media and the Internet?
2. What role does social media play in how we think and act?
3. How can the Internet be used to promote equity and help prevent cyberviolence?
4. How can we balance what the Internet does for us and cyber violence occurring on its platforms?
5. Who produces digital and online content, and why do they do it?
5. 8. How is it that data is never fully deleted on the Internet? Do you think this is a good or bad thing?

6. 9. Do you think your role and your work has a responsibility to prevent cyberviolence on digital platforms?

7. 10. If you could ask us one question about the Internet what would it be?

Strategy Impact

Every media project or story changes some aspect of the world. Digital storytelling and online vlogs are important technological strategies because the most meaningful stories come from people with lived experiences of the issues. By giving young women a voice, stories can help move the needle on community issues by helping other young people to:

- Be aware of the need
- Care about the issue
- Understand the problem and solutions
- Feel a sense of urgency
- Know how to support and intervene

The PSYAC are interested in using digital storytelling methods and vlogs to create and share stories that send a powerful message and educational tools to other youth as well as social media platforms. They frequently referenced *It Starts with You, It Stays with Him* developed by White Ribbon Canada and Le Centre ontarien de prevention des aggressions as a good example of using this type of technological and social media strategy. They appreciated how these videos and stories were used as classroom education tools to prompt discussion on topics such as societal pressures for young men and boys; the importance of gender equality and the impact of violence against women and girls (and men and boys); and homophobia. The PSYAC understood the possibilities for using this type of medium to talk about cyberviolence to other youth, but to also create narratives and discussion around social media platforms and technologies.

(It Starts with You. It Stays with Him: Screenshot, itstartswithyou.ca)
Strategy 2: Mapping a “Violence Free” Social Media Network

Strategy Possibility

The PSYAC was interested in what a “utopian” social media platform would like, that is a platform that was free of cyberviolence and attained equity and diversity amongst its users. We spent some time discussing if this would be a possible strategy if not in actual development but at least theoretically. We wondered what it would like to map out our own social media platform, and how this mapping from young women’s perspective could help social media platforms re-think their own platform design.

The PSYAC spoke about different aspects and characteristics involved in creating a social media platform such as: what a violence free social media platform would look like and what type of policies and features it would need. We used examples of different well-known and popular platforms and social media sites as a starting point. We discussed which ones we liked the most, what tools and aspects we appreciated and what we found to be problematic. While we didn’t get to fully dissect this particular strategy it was definitely helpful in allowing us to theoretically think outside of the box and to help us understand what parts of social media sites we do like and find empowering as well as what aspects we find problematic or that facilitate cyber and sexual violence online. The PSYAC thought it would be incredibly beneficial to create a social media platform map that technology experts could use in the development of their platforms. For this strategy we looked to MyDigitalFootPrint.org: Young People and the Proprietary Ecology of Everyday Data, as a model for possibilities and implications. MyDigitalFootprint.org is a youth-led participatory project from the United States, where young people came together to create their own open source social media network to research the everyday interests and concerns of young people growing up in digital environments. While this project was not specific to cyberviolence it highlighted many cross-sectoral issues such as data, privacy, surveillance and censorship from a youth-led perspective.

Strategy Impact

What would a violence free social media platform look like from a youth’s perspectives? What are the technological possibilities of platforms? How do youth understand social media platforms governance and policy structures? These are just a few of the questions the PSYAC would like to deconstruct. The PSYAC are interested in creating a map of what a ‘violence free’ social media network would look like and this could be used as a tool by social media technologies and companies who want to develop platforms with youth’s voices and experiences in mind. While our youth advisory committee doesn’t necessarily have the skill-set to build their own social media platform they do think it would be interesting to connect with project partners who build platforms and could help the PSYAC map out some key aspects of what it takes to build a social media platform and how could we do it in a way that helps to prevent cyberviolence. A few areas of concern were: privacy terms and agreements, private messenger apps, gender and sex fields, privacy settings and updates, content flagging and moderation, and marketing.
Strategy 3: Online Platform Toolkit (or Code of Conduct)

Strategy Possibility

Of the three different ideas for strategy development the Code of Conduct was the most controversial because the PSYAC were not sure how to feel about the possibility of engaging in structures of surveillance or policing. The PSYAC were adamant that they wanted the possibility of creating a toolkit without the possibility of reproducing hierarchies and policing tactics that they have identified are often used to shame young women and other young folks on the Internet.

In their opinion a Code of Conduct sounds too much like a set of rules and does not do justice to the complexities of experiences that young women are having online, they did not want to create a strategy that would serve to further isolate young people who are already being victimized online.

Instead, they prefer the creating of an online and ever expanding resource or toolkit made for youth and by youth that could inform and engage other young people in both the possibilities and harms of being a young women or person online who are constantly interacting with systems and violence within these spaces. They also saw this as a possibility to create a toolkit or code of conduct for technology platforms themselves. They realize that while there are many different types of platforms and apps and creating specific toolkits and codes of conducts for each one would be impossible, they do like the idea of having a more general toolkit or resource for online platforms to use as a set of guiding intentions and ethics.

The PSYAC spoke about the latest WAM report on Twitter Harassment and thought it would be helpful to have a similar type of document meant for social media platforms more broadly. They felt like they could divide it into different types of apps and technologies and develop sections based on the emerging themes we identified throughout the needs assessment such as policy, governance, privacy, safety, flagging, content moderation, reporting guidelines, authorized reporting, harassment review protocols, user information, evidence collection, account suspension, etc.

Strategy Impact

The PSYAC felt like developing a resource or toolkit aimed both at young women and technology platforms would be a highly effective strategy to help prevent and end cyber and sexual violence. They felt that a resource kit aimed at social media platforms more broadly could help technology folks to understand their perspectives and experiences when it comes to being young women online. They also felt like it could be a good educational tool as well as a tool that could foster accountability and transparency from social media platforms. For the PSYAC it’s not enough to continually tell young women they must stay safe online, they want technology platforms to be understand their experiences and to ensure they are creating platforms with young women in mind.
**Bibliography**


*DIY Guide To Feminist Cybersafety*. [https://tech.safehubcollective.org/cybersecurity/](https://tech.safehubcollective.org/cybersecurity/)


MTV-Associated Press Poll Digital Abuse Survey (2011). (Dataset available through www.knowledgenetworks.com; executive summary available at:


Take Back the Tech. https://www.takebackthetech.net/mapit/


Appendix A: Take Back the Tech’s Ten Tips for Challenging Internet Based Gender Discrimination and Online Harassment Against Women

From: https://www.takebackthetech.net/blog/10-tips-challenging-Internet-based-gender-discrimination-and-online-harassment-against-women

Author: Brindusa Luciana Grosu - YouAct member, Romania

If you know how to use the technology, you can avoid becoming a victim. Before speaking out, it is important to take your time to understand the way the Internet works.

1. **If you intended to be anonymous, stay anonymous.**

In the online world the mere desire of remaining anonymous is not enough to keep your identity safe and hidden. It is not only about avoiding to sign a post or article with your name, many other “clues” can reveal your true identity and thus put you in danger: the website(s) where you posted your story, the social media profiles you used to promote it, your friends who commented on it, the factual information you provided into the story...Staying anonymous is indeed first and foremost a matter of good planning. Think twice about the way you share information and whom you share it with. However, once fully anonymous, don't be afraid to speak your mind and denounce injustice.

2. **If you don't want comments, there is probably an option to disable them.**

Hate speech is annoying but sometimes you can simply turn it off. Read carefully your settings and if you don't want to know what other people think about your story, simply disable the comments option. You can leave an email address for those who really want to contact you. Turning off comments is not cowardice; it can give you peace of mind and the time needed to come to terms with whatever you have to share with the world. If in doubt about your capacity to cope with hate, turn off comments and turn on sincerity mode. It will eventually pay off.

3. **If you didn't mean to share it, but you did, know what to expect.**

Sharing by mistake your story with persons you didn't want to see it, can obviously lead to a tsunami of remarks and threats. That’s why it’s important to pay more attention before hitting the “submit” button. And don't be afraid to face those who try to discourage you. Even when it gets tough, it is important to remember there is always an audience: the other Internet users. The way you respond reveals your level of maturity and confidence, so always aim for fairness and diplomacy.

4. **Don't bother to reply. Don't get into an argument.**

Insulting the person who insulted you will only wear off the difference between the aggressor and you. Not to mention that what you put online tends to stay online, so a moment of anger may cost you more than you think in terms of personal and professional relationships. Let the haters talk by themselves and the public will get the message.
5. Expose the abuse.
You can however publish the hateful remarks and even reveal the identity of the persons who made them. You can always contact the media or ask other bloggers to write about it. You can even start a new online campaign, collecting misogynist remarks from several women activists and putting them together in a “Book of Shame”.

6. Don't rely on words only, especially if you are the target of verbal attacks.
If they spam you with ugly words, look for creative ways to respond. Draw, sing, dance or take it back to the offline world with a symbolic flash-mob or happening. It takes different skills to combat hate, so dare to be imaginative and stand out.

7. Keep your sense of humor.
The unequal power relationship tends to block the victim into an emotional situation where she is no longer allowed to express humor, because she is the one being mocked. Nevertheless, you can be the first to use humor and confident self-irony. It is actually much harder to criticize someone who is funny. New artsy apps and software can help you put together collages, caricatures, manga or digital photos in order to express a whole range of situations from absurd to paradoxical.

Last, but not least, the Internet is not everything and it is ultimately the offline world which matters most. Whichever the fails or successes, remember there is always another level to take it to: your surrounding reality.

8. Remember the 99% who are not online.
If you are praised online, think that just around the corner there might be extremists ready to attack you. If you are spammed, remember all those persons who think alike you and would support your cause if they had access to the Internet. The online world is but a small fragment of reality. Only real-world action can lead to lasting changes.

9. Don't hesitate to meet in person your supporters.
Alliance-building cannot and should not be only web-based. Face-to-face meetings make a community stronger and might give you the chance to share effective online activism strategies. Even if it is tempting to count you Facebook likes and feel all-powerful at your desk, do find the time to actually meet the 2-3 persons who showed deep commitment to your cause...especially if they know code!

10. Real-life stories move the virtual world.
Clever opinion pieces and well-researched papers can help a cause move forward, nevertheless busy people tend to begin and end their day by reading diaries, personal accounts and real-life stories. Knowing this, feel proud if your entry awakened many controversial views. It only means a lot of persons read it. Some wrote back, some didn't. Some said nasty things, some encouraged you. Freedom of speech is a common right we all share, but being listened to is a privilege. So if your story made waves, keep trying to move mountains.
Appendix B: TrollBusters


Offering pest control solutions for women publishers

International Women’s Media Foundation Hackathon, January 30, 2015, New York City

Dr. Michelle Ferrier, Sneha Inguva, Debbie Galant, Berta Valle, Louisa Reynolds
Online Harassment: 40% and growing

- Women publishers experience cyberbullying on their sites.
- General news sites have struggled with moderating online commenting.

Women Live Online and That’s Where They Find Us
Women Journalists Are Targeted Online

What We Offer

- **S.O.S. Team**: Countering cyberattacks in real-time with online community support and positive messaging.

- **RAID**: Finding and outing trolls online and tracking where they operate using network analysis technologies.

- **SUPPORT**: Providing technical, legal services and psychological services; resources for publishers under denial of service attacks.
S.O.S. Team: Just-in-Time “Attagirls”

- Users who report personal harassment are supported online with users from their communities.
- Push alerts go to people in their networks.
- Positive messaging and endorsements combat negative comments.
RAID: Community Clustering

Using a proprietary technology for network analysis developed by Ohio University students, we find and aggregate communities of trolls and identify who else is a subject of attack.

C.A.T.S.: Clustering Analysis and Targeting System, Ohio University

Also Fighting This Battle

- **Trolldor** | A global blacklist of Twitter trolls
- **NoBullying.com** | Educational resources
- **Southern Poverty Law Center** | Map of hate groups
- **No Hate Speech** | Social media against cyberbullying
- **Cyberbullying.us** | Research on cyberbullying
- **Committee to Protect Journalists** | Fights efforts to intimidate newsgatherers
- **iHollaback** | Fighting catcalling on the streets
- **Megan Meier Foundation** | Fighting childhood bullying
How We’re Different

- **We help victims of cyberbullying in real time** by having our community leave supportive comments at the point of bullying.

- **We track top trolls and their nests** – *out of their sight* – for a verified community of users who have pledged not to engage in or ignore hate speech.

- **We gather all the resources** in one place.

### TrollBusters: Our Team

- Dr. Michelle Ferrier, U.S.A.
- Sneha Inguva, Indian American
- Debbie Galant, U.S.A.
- Berta Valle, Nicaragua
- Louisa Reynolds, United Kingdom

*Offering pest control solutions for women publishers*