Centre for International
Governance Innovation

Supporting a Safer Internet Paper No. 1

Technology-Facilitated Gender-Based Violence

An Overview

Suzie Dunn

Centre for International
Governance Innovation

Supporting a Safer Internet Paper No. 1

Technology-Facilitated Gender-Based Violence

An Overview

Suzie Dunn

About CIGI

The Centre for International Governance Innovation (CIGI) is an independent, non-partisan think tank whose peer-reviewed research and trusted analysis influence policy makers to innovate. Our global network of multidisciplinary researchers and strategic partnerships provide policy solutions for the digital era with one goal: to improve people's lives everywhere. Headquartered in Waterloo, Canada, CIGI has received support from the Government of Canada, the Government of Ontario and founder Jim Balsillie.

À propos du CIGI

Le Centre pour l'innovation dans la gouvernance internationale (CIGI) est un groupe de réflexion indépendant et non partisan dont les recherches évaluées par des pairs et les analyses fiables incitent les décideurs à innover. Grâce à son réseau mondial de chercheurs pluridisciplinaires et de partenariats stratégiques, le CIGI offre des solutions politiques adaptées à l'ère numérique dans le seul but d'améliorer la vie des gens du monde entier. Le CIGI, dont le siège se trouve à Waterloo, au Canada, bénéficie du soutien du gouvernement du Canada, du gouvernement de l'Ontario et de son fondateur, Jim Balsillie.

Credits

Managing Director & General Counsel Aaron Shull
Manager, Government Affairs and Partnerships Liliana Araujo
Publications Editor Susan Bubak
Publications Editor Lynn Schellenberg
Graphic Designer Abhilasha Dewan

For publications enquiries, please contact publications@cigionline.org.

This work was carried out with the aid of a grant from the International Development Research Centre, Ottawa, Canada.

The views expressed herein do not necessarily represent those of IDRC or its Board of Governors.

Printed in Canada on Forest Stewardship Council® certified paper containing 100% post-consumer fibre.

67 Erb Street West
Waterloo, ON, Canada N2L 6C2
www.cigionline.org

Table of Contents

About the Author

Suzie Dunn is a senior fellow at CIGI, and a Ph.D. candidate and part-time professor at the University of Ottawa's Faculty of Law. She currently teaches Contracts Law and the Law of Images at the university and regularly guest lectures on law and technology. Her research centres on the intersections of gender, equality, technology and the law, with a specific focus on the non-consensual distribution of intimate images, deepfakes and impersonation in digital spaces. As a subject matter expert on online gender-based violence, Suzie is contributing to Supporting a Safer Internet: Global Survey of Gender-Based Violence Online, a two-year research project supported by the International Development Research Centre.

As an innovative thinker with a deep passion for equality and technology, Suzie has published and presented her work both nationally and internationally on issues including the importance of internet connectivity for Northern youth, the application of Canadian law to deepfake technology and civil responses to the non-consensual distribution of intimate images. She is also a researcher with The eQuality Project, where she is developing a case law database on criminal law decisions involving technology-facilitated violence.

In 2018, as a policy adviser with Global Affairs Canada's Digital Inclusion Lab, Suzie contributed to drafting two international commitments to end gender-based violence in digital contexts: the Group of Seven's "Charlevoix Commitment to End Sexual and Gender-Based Violence, Abuse and Harassment in Digital Contexts" and the United Nations Human Rights Council's resolution entitled "Accelerating efforts to eliminate violence against women and girls: preventing and responding to violence against women and girls in digital contexts," both of which were adopted that year.

About the Project

Supporting a Safer Internet: Global Survey of Gender-Based Violence Online is a two-year research project, in partnership with the International Development Research Centre (IDRC) and Ipsos. This project explores the prevalence of online gender-based violence (OGBV) experienced by women and LGBTQ+ individuals in the Global South. From cyberstalking, impersonation and the non-consensual distribution of intimate images, to deliberate personal attacks on communications channels, OGBV is silencing the voices of women and LGBTQ+ individuals, causing digital exclusion and propagating systemic inequalities. To address these emerging challenges, the survey and papers produced under this research initiative will help to develop policy recommendations and navigate shared governance issues that are integral to designing responses to OGBV — whether that be through the regulation of online social media platforms, educational programming or legal recourse.

Acronyms and Abbreviations

APC	Association for Progressive Communications
CIGI	Centre for International Governance Innovation
COVID-19	coronavirus disease 2019
GPS	Global Positioning System
ICT	information and communications technology
IDRC	International Development Research Centre
LGBTQ+	lesbian, gay, bisexual, transgender and questioning
MPs	members of Parliament
MRAs	men's rights activists
OGBV	online gender-based violence
PTSD	post-traumatic stress disorder
TFGBV	technology-facilitated gender-based violence
UN OHCHR	United Nations Office of the High Commissioner for Human Rights

Executive Summary

Technology-facilitated gender-based violence (TFGBV) is a complex worldwide phenomenon with devastating results. Research to date shows that victim-survivors of intimate partner violence are tracked by their abusive partners who use technology to monitor their movements and communication. Many women journalists, human rights defenders and politicians face daily death threats and rape threats for speaking out about equality issues or for simply being a woman in a leadership role. Those with intersecting marginalized identities are at specific risk, with Black, Indigenous and people of colour; lesbian, gay, bisexual, transgender and questioning (LGBTQ+) people; and people with disabilities facing higher rates of attacks as well as concerted attacks that specifically target their identities. These attacks create legitimate safety concerns, involve egregious invasions of privacy and can have significant financial costs for those targeted; however, one of the most serious impacts is the silencing of women's and LGBTQ+ people's voices in digital spaces. TFGBV makes it unsafe and unwelcoming for women and LGBTQ+ people to express themselves freely in a world where digital communication has become one of the primary modes of communication, particularly during the coronavirus disease 2019 (COVID-19) pandemic.

As a fairly new phenomenon, TFGBV is not generally well understood. There has been relatively little empirical research conducted on TFGBV, and the bulk of the research on this topic to date is focused on higher-income countries. To better understand TFGBV, the Centre for International Governance Innovation (CIGI) and the International Development Research Centre (IDRC) have embarked on a two-year research project entitled Supporting a Safer Internet: Global Survey of Gender-based Violence Online in order to examine women's and LGBTQ+ people's experiences with technology-facilitated violence globally. In 2021, this project will survey representative samples of people in 18 countries, the majority of which are lower- and middle-income countries, to learn about people's experiences with TFGBV in these regions. The goal of this research is to specifically learn more about the experiences of people in the Global South, where there is a dearth of empirical data on TFGBV.

As the first publication in this series, this paper serves as an introduction to TFGBV and many of the concepts that will serve as the basis for this research project. Relying on the research done to date on TFGBV, this paper reviews some of the more common forms of TFGBV, including harassment, image-based sexual abuse, publication of personal information, doxing, stalking, impersonation, threats and hate speech. Following this review, the paper notes who is at greatest risk of being targeted by TFGBV, including victim-survivors of intimate partner violence, women in leadership positions, and women and LGBTQ+ people with intersecting marginalized equality factors. Finally, it highlights research that has identified the individual and systemic harms of TFGBV, including psychological and emotional effects, privacy and safety concerns, the silencing of women's voices and economic impacts.

Introduction

TFGBV is a modern form of gender-based violence that utilizes digital technologies to cause harms. As these technologies increasingly become mainstays in everyday life, TFGBV has proliferated. Particularly over the last year, with much of people's lives moving online due to the COVID-19 pandemic, there has been an increase in TFGBV (UN Women 2020a). Like other forms of gender-based violence, TFGBV is rooted in discriminatory beliefs and institutions that reinforce sexist gender norms. It intersects with racism, homophobia, transphobia, ableism and other discriminatory systems in many of its manifestations. As a relatively new phenomenon, there is a small but growing collection of research on this topic, including several emperical studies (for example, see Plan International 2020; Henry et al. 2020; Gurumurthy, Vasudevan and Chami 2019; Amnesty International 2018). This burgeoning research makes it clear that TFGBV is a growing problem internationally. However, there is a general need for more research to understand this issue more broadly, and a pressing need in particular for further research in lower- and middle-income countries, as current research is dominated by perspectives from higher-income countries (Iyer, Nyamwire and Nabulega 2020).

In order to contribute to this research area, CIGI and the IDRC have embarked on a two-year research project entitled Supporting a Safer Internet: Global Survey of Gender-Based Violence Online in order to examine women's and LGBTQ+ people's experiences with technology-facilitated violence globally. CIGI is an independent, non-partisan think tank that produces peer-reviewed research intended to be used by policy makers internationally. The IDRC is a Canadian Crown corporation that funds research that supports large-scale positive change in developing countries.

In 2021, this project will survey representative samples of individuals from 18 countries, the majority of which are lower- and middle-income countries, to learn about people's experiences with TFGBV in these regions. Using this data, and in partnership with regional experts, this project will produce several research papers on TFGBV that will prove useful for policy makers, civil society organizations and others interested in gaining a better understanding of TFGBV. One of the primary goals of this project is to learn more about the experiences of people in the Global South, where there is a dearth of empirical data on TFGBV. As part of this research project, this paper serves as an introduction to the concept of TFGBV as it is currently understood within existing literature. It will discuss trends, review existing research, and outline relevant concepts and terms that will be used to inform CIGI's and the IDRC's ongoing research on TFGBV. The project's authors hope that this research will help people and policy makers better understand the breadth and impact of TFGBV.

This paper will canvass research from multiple countries. However, it should be noted that much of the current literature on TFGBV is focused on the perspectives of women and girls in higher-income countries. Additionally, due to the language limitations of the author, the research for this paper was limited to literature and reports written in English. For this project, CIGI and the IDRC are working with experts in additional countries and will be producing further research that will expand its examination beyond what is available in the English language. The author would like to acknowledge the valuable research being done globally by organizations invested in understanding and ending TFGBV in other languages that the author was unable to highlight in this paper.

Gender-Based Violence

Gender-based violence is a global phenomenon that violates women's and girls' international human rights (UN 2017). Across the world, women and girls face unacceptable rates of violence at the hands of their intimate partners (World Health Organization 2013), something that has only increased since the COVID-19-related lockdowns in 2020 (UN Women 2020a). Statistically, women and girls are more likely to be stalked (Milligan 2011; Baum et al. 2012; Staude-Müller, Hansen and Voss 2012) and murdered (World Health Organization 2013) by their intimate partners than men, and regardless of where they live in the world, they face a high likelihood of experiencing sexualized violence throughout their lives (ibid.). While in public, at social events or in the workplace, they have been subjected to unwanted sexual harassment in disproportionate numbers (Backhouse 2012; Vera-Gray and Kelly 2020). Those living in areas impacted by violent conflict and war are targeted with gendered violence and rape (Wood 2018). These are just some examples of how gender-based violence can be an everyday occurrence for many women and girls.

In sheer numbers, women and girls remain the primary targets of gender-based violence. However, despite the focus on cis-women and girls in most research on gender-based violence, it is not only cis-women and girls who are harmed by gender-based violence. Emerging research shows that transgender, non-binary and gender-nonconforming people (Wirtz et al. 2018),[1] as well as men who fall outside patriarchal norms of masculinity, such as gay men, are harmed by gender-based violence (Evens et al. 2019). These individuals are targeted due to their gender nonconformity, gender expression and gender identity (Wirtz et al. 2018). Statistics on these groups show they face significant levels of harassment, physical attacks and sexual assaults due to their gender identity and expression (James et al. 2015; Evens et al. 2019). As gender-based violence is rooted in the systemic reinforcement of gender norms and inequality, it is important to recognize how it affects these groups as well as cis-women and girls.

1 For this paper, the term "transgender" will refer to people whose birth sex does not match their gender identity, including transgender, gender-nonconforming and non-binary people.

TFGBV

As people's lives become increasingly digitally mediated (UN Women 2020b), gender-based violence has likewise shifted to the digital realm (Woodlock 2015). Perpetrators of TFGBV have adopted the tools of technology to broaden the scope of violence they enact against their victims (Freed et al. 2017). Whether it be intimate partner violence, gender-based harassment, hate campaigns or misinformation campaigns, technology is now being used by abusers to further these harms (European Institute for Gender Equality 2017). Digital technologies have simplified well-known abusive behaviours, such as stalking (Khoo, Robertson and Deibert 2019) and child luring (Van der Wilk 2018) by providing convenient tools for abusers to access their targets. Additionally, they have opened the door to new forms of abuse that require technology, such as the non-consensual creation of sexual images of women through artificial intelligence (i.e., sexual deepfake videos or virtual reality pornography) (Dunn 2020). Systemic sexism is also being reinforced online. In recent years, communities have developed on messaging fora, group messaging apps and social media websites, where people actively share and amplify sexist, hateful and violent ideas about women, girls and transgender people (Baele, Brace and Coan 2019). Unfortunately, as with the increase in COVID-19-related domestic violence, there has also been an uptick in TFGBV in 2020 as people are required to engage more often online (UN Women 2020a).

Dubravka Šimonović, the UN Special Rapporteur on violence against women, its causes and consequences, noted that these modern forms of violence must be understood within the broader scope of gender-based violence (UN 2018). They exist on the continuum of gender-based violence and are often enacted in tandem with other, more familiar, forms of gender-based violence, such as physical violence in domestic relationships (Dragiewicz et al. 2018). Azmina Dhrodia (2018, 381), who has conducted extensive research on gender-based harassment on social media, has stated that "the widespread inequality and discrimination against women that remains embedded in society is increasingly replicated online. Acts of violence and abuse against women online are an extension of these acts offline." At present, women and girls cannot escape sexism, misogyny or gender-based violence in digital spaces

(United Nations Office of the High Commissioner for Human Rights [UN OHCHR] 2017).

As a novel manifestation of gender-based violence, there are some factors that make TFGBV particularly unique, including the possibility for cross-jurisdictional abuse, the ability for abusers to remain anonymous, the constant access to the survivor through connected devices, the perpetual nature of digital content, the ease with which content can be copied, the breadth of audiences witnessing the abuse and the opportunities for abusers to join forces on digital platforms to organize attacks.

Unlike physical violence, which requires people to be in the same place, technology-facilitated violence can happen across geographical locations, with abusers being able to access their victims even when they are not in close physical proximity (Bailey and Mathen 2019). Abusers can target people in different cities or countries and can do so under the cloak of anonymity (Council of Europe 2018). This can cause problems for law enforcement investigating these crimes (Dunn, Lalonde and Bailey 2017) and can make it difficult to assess the risk of violence when the abuser is an anonymous person on the internet (Inter-Parliamentary Union 2016). Additionally, it can be impossible for victim-survivors to escape TFGBV, even when at home, if the violence is occurring on social media platforms accessible on the target's phone or computer, or if the abuser has remote access to her devices (Association for Progressive Communications [APC] 2012).

The versatile nature of digital communication also causes problems. In many cases, there is a permanent digital record of the abusive content that is difficult to avoid and may be accessible worldwide (Van der Wilk 2018). This is particularly relevant when private images or information has been shared online in harmful ways, because even if the original source of the information is deleted, copies of the information may have been downloaded and can be redistributed at any time, leaving the victim-survivor at perpetual risk of future abuse (Goldberg 2019). Further, the internet also provides spaces for groups of abusers to coordinate and promote large-scale attacks against particular individuals or groups (Salter 2017). These online mobs can overwhelm their targets with a constant deluge of harassment and have driven many women away from participating in digital spaces (Plan International 2020).

Research has repeatedly demonstrated the severe effects TFGBV can have on the lives of those impacted by it (Woodlock 2015). Yet this form of violence is viewed by many as insignificant because it occurs in digital spaces (Veletsianos et al. 2018). As with sexual harassment before it, many forms of TFGBV are still not understood as gender-based violence by the wider public or the justice system (Dunn, forthcoming 2021). It is minimized because of the mistaken belief that online abuse cannot be as genuinely harmful as abuse that happens in the physical world (Fairbairn 2015; West 2014). As a result, victim-survivors have been told to ignore the abuse or just disconnect from social media or their devices to avoid being abused (Citron 2014), something that is an impossibility for many people in the modern world. The need for internet connectivity is only becoming more relevant during the COVID-19 pandemic, where much of people's work and social and political lives are being coordinated online. In some countries, important public discourse and basic governmental and civil society services are only accessible via the internet. Disconnecting is not a viable solution for most people and does not realistically mitigate the harms caused by TFGBV.

Victim-survivors of TFGBV should have the violence against them taken seriously and be provided meaningful strategies to prevent this violence (Dunn, Lalonde and Bailey 2017). At present, there are few avenues of support for victim-survivors of TFGBV. When it released its annual Web index for 2014–2015, the World Wide Web Foundation (2014) reported that of the 86 countries it surveyed, 74 percent of their legal systems were not appropriately responding to TFGBV. In 10 countries across Africa, Asia and Latin America,[2] the Women's Rights Online (2016) network found that there were few mechanisms available for women to report this abuse. Where there were some mechanisms, the police and judicial systems lacked the ability to effectively respond to TFGBV. Policy makers ought to be considering how to support legal, educational and civil society responses that could better address TFGBV.

In the following three sections, this paper will introduce the reader to some of the more salient concepts associated with TFGBV. Based on existing research, the first section will outline several

2 Colombia, Egypt, Ghana, India, Indonesia, Kenya, Mozambique, Nigeria, the Philippines and Uganda.

forms of TFGBV. This section covers many of the more common forms of TFGBV violence but is in no way meant to be an exhaustive list of all forms of TFGBV. As technology evolves, perpetrators of gender-based violence will find novel ways to use technology to cause harms, and there are a multitude of ways technology can be abused. The examples provided focus on the behaviours that have been identified in existing research.

The second section will look at who is impacted by TFGBV. Research shows that this is a gendered phenomenon that greatly impacts women in abusive intimate relationships, but it is also an intersectional one. Women, girls and transgender individuals cannot separate their gender identity from other identity factors such as sexual orientation, race or ability (Collins 1990). Their intersecting social locations will impact the quality and volume of the TFGBV that they experience (Plan International 2020). This section will highlight some of the research that shows that women and transgender people who are Black, Indigenous, women of "colour" members of the LGBTQ+ community and/or disabled are uniquely targeted. Moreover, if a woman is in a leadership role, such as a journalist, politician or human rights defender, she will be at increased risk of experiencing TFGBV. This section will review existing research that shows how these groups of women are particularly at risk of being targeted by TFGBV.

The third section will discuss some of the individual and systemic harms that have been associated with TFGBV, including psychological harms, privacy violations, safety concerns, limitations on speech and economic harms.

Forms of TFGBV

The UN (1993, article 1) Declaration on the Elimination of Violence Against Women defines gender-based violence as any act "that results in, or is likely to result in, physical, sexual or psychological harm or suffering to women, including threats of such acts, coercion or arbitrary deprivation of liberty, whether occurring in public or private life." For the purposes of this paper, the author expands this definition of gender-based violence to include transgender, non-binary and gender-nonconforming individuals who experience violence due to sexism and the reinforcement of patriarchal gender norms. TFGBV is any form of gender-based violence that involves the use of digital technologies.

While technology can be used in a variety of ways to enact violence, there have been some clear trends in the problematic way technology is being used (APC 2011). In 2018, the United Nations released the *Report of the Special Rapporteur on violence against women, its causes and consequences on online violence against women and girls from a human rights perspective* (UN 2018). This report highlighted many of the ways in which technologies are being used to perpetrate violence against women and girls. After receiving reports on TFGBV from across the globe, the Special Rapporteur identified multiple forms of TFGBV included threats, inciting gender-based violence, harassing digital communication, dissemination of harmful lies, impersonation, trafficking of women, disclosing private information (or threatening to do so), doxing, sextortion, trolling, unauthorized access to information or devices, manipulated images, mobbing (or networked harassment) and stalking.

Relying on this report and other relevant research, the following section reviews a selection of the more common forms of TFGBV, including harassment, networked harassment, image-based sexual abuse, the public disclosure of private information, defamation, stalking, impersonation, threats and hate speech.[3] Each of these forms of TFGBV has its own unique markers, but many of these behaviours overlap with each other. For example, someone may harass another person by creating a nude image of them and posting it on a fake profile along with their target's contact information, incorporating image-based sexual abuse, the release of private information, impersonation and harassment.

Harassment

Harassment encompasses a variety of unwanted digital communication (Duggan 2017; Digital Rights Foundation 2018). It can involve a brief incident, such as a single targeted racist or sexist comment (Lenhart et al. 2016), or a long-term organized attack, such as the Gamergate campaign.

3 It should be noted that issues specifically dealing with children, including child luring and child sexual abuse material, were not included in this paper as CIGI will not be surveying children. Human trafficking was also outside the scope of this research.

During the Gamergate attacks, large groups of sexist gamers organized to target certain female videogame developers and media critics. These abusers suggested the women used their sexuality to advance in the gaming world or stated that their gendered critiques were unwelcome in the community. Over multiple years, the abusers discredited the women's work, sent them death threats and gamified their harassment toward these women (Massanari 2017). While large-scale attacks like these are easily identifiable as harassment, smaller-scale actions with harmful effects must be identified as harassment as well. In its 2016 report on online harassment, Data & Society stated that "online harassment is defined less by the specific behavior than its intended effect on and the way it is experienced by its target" (Lenhart et al. 2016). Online harassment is known to cause the recipient mental distress and sometimes fear (Citron 2014).

Women and girls experience high levels of harassment online, and that harassment is typically focused on their gender. In Kenya, a study by the African Development Bank Group (2016) on TFGBV found that most victims of online harassment were women. Amnesty International's (2018) report on online harassment on Twitter, *Toxic Twitter*, found that a person's social location, such as their gender or race, were often targeted when they were harassed online. Further, their research showed that "nearly a quarter (23%) of the women surveyed across the eight countries said they had experienced online abuse or harassment at least once, including 21% of women polled in the UK and 1/3 (33%) of women polled in the US. In both countries, 59% of women who experienced abuse or harassment [on Twitter] said the perpetrators were complete strangers" (ibid., 23). Harassment can come from people known to the victim-survivor or from strangers. For example, abusive intimate partners in Canada have been known to harass their partners via technology, both within an existing relationship and following a breakup (West 2014). In West Bengal, women reported being harassed by "wrong numbers," which is when they receive "unrelenting phone calls from unknown men" who sexually harass them (Udwadia and Grewal 2019).

For victim-survivors of TFGBV, the harassment against them is often gendered or sexualized (Henry and Powell 2016). A study from Southern India surveyed 881 women in college and found that 83 percent of those women who had faced online harassment experienced sexual harassment, such as abusers manipulating their images to appear sexual, sharing their sexual images without consent and making relentless unwanted requests for sexual contact (Gurumurthy, Vasudevan and Chami 2019). Reinforcing gender roles also played a part in attacks against these women. Some were "mob-led castigation[s] of 'defiant' women" (ibid., 6), and others targeted non-heteronormative women and transwomen in an effort to "gendertroll" them. A similar trend was found in Ethiopia, Kenya, Senegal, South Africa and Uganda where, of the 28.2 percent of women who had experienced online harassment, 36 percent of this harassment was sexual and 33.2 percent of it was unwanted sexual advances and offensive name calling (Iyer, Nyamwire and Nabulega 2020).

In 2014, the Pew Research Center's study on online harassment in the United States found that men were more likely to experience name calling or have embarrassing comments made toward them, whereas women were more likely to have experienced more severe forms of harassment such as sexual harassment and stalking (Duggan 2014). A 2017 study by the same organization confirmed that women face sexual harassment online at much higher rates than men. It also found that women received unsolicited or unwanted sexual images at a higher rate than men and were twice as likely as men to report their most recent experience with online harassment to be extremely or very upsetting (Duggan 2017).

As will be discussed in greater detail below, a person's race, ability, ethnicity, caste, sexual orientation, gender identity, gender expression and immigration status play a central role in TFGBV. Reports show that women with multiple intersectional marginalities face significantly higher rates of online harassment and attacks that target their gender as well as their other identity factors (Amnesty International 2018). In a study from Southern India, 22 percent of women who experienced online harassment had abusers comment on their skin colour (Gurumurthy, Vasudevan and Chami 2019). Plan International (2020) reported that girls and women globally were more likely to be harassed relentlessly if they were identified as LGBTQ+, disabled, racialized or a member of a minority ethnic group. In Canada, Inuit, First Nations and Métis women face some of the highest rates of gender-based violence in the country, and online harassment is part of that violence (Driscol 2020). In Australia, the

eSafety Commissioner (2019) found that some immigrant women experiencing TFGBV faced digital threats of deportation, culturally specific humiliation (i.e., sending images of a woman not wearing her hijab) and threats of so-called honour killings. Disabled women who rely on assistive devices and are in abusive relationships have had their technology destroyed or threatened to be destroyed by abusive partners (Copel 2006). These women's understanding of their gender and their experiences with TFGBV are interwoven with these varying social locations.

Networked Harassment

Harassment can be done by a single person, such as an ex-partner or an online stalker; however, the internet has provided spaces for people to organize and encourage larger-scale coordinated attacks by groups of abusers (Van der Wilk 2018). Alice E. Marwick and Robyn Caplan (2018) describe this type of abuse as "networked harassment," which includes coordinated and organized attacks against particular individuals or issues, such as by groups that target feminists or people who post about racial equality issues online. According to their study, networked harassment against women has been conducted through a loose network of individuals from what Caplan and Marwick call the "manosphere," which is a collection of men's rights activists (MRAs), anti-feminists, pickup artists, alt-right groups, incels (involuntary celibate men), and other groups that hold anti-women and racist views or who seek to reinforce patriarchal gender norms. These groups encourage online harassment against specific people and groups and share discriminatory views on message boards such as Reddit, 4chan and 8chan (Salter and Crofts 2015). For example, Michael Salter and Thomas Crofts (ibid.) have found that groups of misogynistic men have been known to monitor websites that post non-consensually distributed intimate images in order to collectively stalk and harass the women featured in the images.

Networked harassment may include trolling, which is purposely upsetting or disrupting online events, debates or hashtags (UN 2018), and coordinated flagging, which is falsely reporting people to websites in order to get them kicked off a platform, among more common forms of harassment such as derogatory comments about women's bodies or rape threats. Groups also use private messaging sites such as Facebook or WhatsApp to have misogynistic conversations and to share abusive content with each other (Gurumurthy, Vasudevan and Chami 2019; Backhouse, McRae and Iyer 2015). Networked harassment in Ethiopia, Kenya, Senegal, South Africa and Uganda is on the rise, especially among women in leadership roles such as journalists, activists and politicians, with some attacks calling for the murder of particular women (Iyer, Nyamwire and Nabulega 2020). Following the increased use of the video streaming site Zoom due to COVID-19 restrictions, a new trend emerged in networked harassment involving what is known as "Zoom-bombing." Zoom-bombing occurs when people join online gatherings in order to post racist, sexist, pornographic or anti-Semitic content to shock and disturb viewers. Research from Ryerson University's Infoscape Research Lab showed that most Zoom-bombings involved misogynistic, racist or homophobic content (Elmer, Burton and Neville 2020).

Image-Based Sexual Abuse

The non-consensual distribution of intimate images by ex-partners (colloquially known as "revenge porn") is highly reported in the media and is often at the centre of discussions about image-based sexual abuse, including how to regulate it (Valente et al. 2018). However, image-based sexual abuse actually consists of a broad range of abusive behaviours and is perpetrated by a wide range of individuals (McGlynn, Rackley and Houghton 2017). The concept of image-based sexual abuse was developed by UK scholars Claire McGlynn and Erika Rackley (2017), who define it as private sexual images that have been created and/or distributed without the consent of the person featured in them, as well as the threats to create and distribute these images. Below, this paper will review several forms of image-based sexual abuse, including the non-consensual distribution of intimate images, voyeurism/creepshots, sexploitation, sextortion, the documentation or broadcasting of sexual violence, and non-consensually created synthetic sexual media, including sexual deepfakes.

Non-consensual Distribution of Intimate Images

The non-consensual distribution of intimate images, which is often problematically[4] described as revenge porn, occurs when a person's sexual images are shared with a wider than intended audience without the subject's consent (Dunn and Petricone-Westwood 2018). The images are often distributed by an ex-partner who may have consensually received or taken the images during a previous intimate relationship (Henry et al. 2020). A study from Brazil found that more than half of the respondents (60 percent) to its survey had originally authorized or provided the recording to the abuser in the context of a sexual relationship, in some cases due to pressure from the abuser to provide the photos (França and Quevedo 2020). In other cases, the images were obtained without authorization (ibid.). The images were later sent to the victim-survivors' friends, family and co-workers; published on social media pages; and/or posted to public pornography websites, among other places, without the subjects' consent (Henry and Flynn 2019).

While ex-partners are commonly the people who take or distribute sexual images without consent (Aikenhead 2018), abusers have included a wide range of people, including family members, colleagues, friends and strangers (Henry et al. 2020). It is important to note that the abuse does not always stop with the first person who distributes the images without consent. As McGlynn and Rackley (2017) have reported, those further down the chain of distribution, such as individuals who redistribute, view or otherwise engage with these images once they have been initially shared, are also participating in the abuse.

For those who do choose to engage in the non-consensual distribution of intimate images, their motivation can range from a desire to humiliate the other person or harm their reputation, to gain status, to bond with peers, to make a profit or for sexual purposes (Henry et al. 2020). One of the earliest widely reported cases of the non-consensual distribution of intimate images was that of Hunter Moore in the United States. In the early 2010s, Moore ran and profited from the website IsAnyoneUp.com, which solicited and displayed sexual images of other people without their consent. The name, workplace, social media information and the city in which the subject lived were often shared alongside the images, resulting in unwanted exposure, contact and harassment (Henry and Flynn 2019). In this case, Moore was eventually convicted of working with another person to hack into women's accounts to steal nude images of them for content on his website (Slane and Langlois 2018).

A second well-known American case involved the 2014 celebrity nude photo leak, where hackers stealthily and illegally accessed the cloud storage accounts of several prominent, mainly female, Hollywood celebrities in order to copy and publicly post the celebrities' private nude images on messaging boards such as 4chan (Marwick 2017). Many of these women spoke out about the abuse. In an interview with *Vanity Fair*, Jennifer Lawrence described the leak of her images as a "sex crime" and urged people not to view them (*Vanity Fair* 2014). Case studies in Malawi and Uganda have also shown that images that are hacked or stolen from computers have been distributed without consent, and celebrities have been targeted by this form of abuse (Chisala-Tempelhoff and Kirya 2016).

Regardless of the relationship between the abuser and victim-survivor, image-based sexual abuse is a highly gendered phenomenon (Uhl et al. 2018). While some quantitative studies have found that both men and women have had their images shared without their consent, research has demonstrated that the impact on women whose images have been shared has been much more severe (Lenhart et al. 2016; Henry et al. 2020). Further, men are more commonly perpetrators of the distribution (Powell et al. 2018), and sexist commentary often accompanies the woman in the image (Langlois and Slane 2017). A study by Nicola Henry and Asher Flynn (2019) found that the non-consensual postings of intimate images on high-volume websites were predominantly of women; comments on the images appeared to be mainly made by men; and these comments used sexist language that objectified the woman in the image.

The gendered aspect of this type of abuse was further demonstrated in a 2020 study from Australia, New Zealand and the United Kingdom, which found that men were twice as likely to perpetrate image-based abuse compared to women

4 The term "revenge porn" should be avoided. The term "revenge" suggests that the person in the images was deserving of the abusive disclosure of their images, and the term "pornography" suggests that the images may be legitimately used by unintended audiences for sexual purposes.

(Henry et al. 2020). This study found that men were more likely to have engaged in all forms of image-based sexual abuse, including taking, sharing or threatening to share images without consent. Additional research on Canadian criminal case law involving technology-facilitated violence (The eQuality Project 2020) likewise found that many forms of image-based abuse, such as the non-consensual distribution of intimate images and voyeurism, were highly gendered, with criminal perpetrators being nearly exclusively men and the victim-survivors being predominantly women and girls (Bailey and Mathen 2019; Bailey 2020).

Troublingly, sharing and commenting on these images has been found to be a form of peer bonding for some men and is quite normalized in modern society (Gurumurthy, Vasudevan and Chami 2019). In their research on non-consensually distributed intimate images, Walter S. DeKeseredy and Martin D. Schwartz (2016) found that, in many cases, sharing and commenting on image-based sexual abuse was used as a way to connect with other men in displays of hypermasculinity. A 2017 study by Matthew Hall and Jeff Hearn (2017) showed that comments about the non-consensually distributed intimate images are regularly misogynistic.

On a systemic level, the non-consensual distribution of intimate images has been used to reinforce gender norms and assert male domination. In Southern India, the non-consensual sharing of sexual images was used to normalize men's sexual domination over women's bodies (Gurumurthy, Vasudevan and Chami 2019). Research from Malawi and Uganda noted that women who have their images shared without their consent are vilified and labelled as "sluts" for transgressing strict patriarchal norms around sexuality (Chisala-Tempelhoff and Kirya 2016). In Zimbabwe, patriarchal belief systems were reinforced through this type of image sharing and normalized the non-consensual distribution of intimate images by disgruntled male ex-partners or men who were sexually rejected by women (Mafa, Kang'ethe and Chikadzi 2020). These non-consensually shared images not only hurt the targeted individual but maintain sexist social hierarchies.

Voyeurism/Creepshots

Voyeurism is defined as a person surreptitiously taking photos or recording a video of another person for a sexual purpose (Citron 2019). Voyeurs use hidden cameras to secretly take photos of the victim-survivor without their knowledge, in some cases livestreaming the recorded images to an undesired audience (Waldman 2017). The images may be captured by a camera hidden in a private place, such as in a washroom or changeroom, or the images may be taken in public places using discreet photography techniques, such as by using cameras hidden in everyday objects, using a zoom lens or taking photos when someone is not paying attention. Some voyeurs will try to take pictures up a woman's skirt or down her shirt without her being aware of it, a practice known as "upskirting" or "downblousing" (McGlynn, Rackley and Houghton 2017). These images may be kept for personal use (Thomasen and Dunn, forthcoming 2021) or shared on public websites (Henry and Flynn 2019).

As miniaturized cameras have become more accessible and affordable, this behaviour has spread widely. In South Korea, the voyeuristic use of hidden cameras in public has become so prevalent, it has been described as an "epidemic" by some news outlets. It has been reported that hidden cameras used to sexually spy on women are so common that many women in that country feel the need to check for cameras in public washrooms and hotel rooms before feeling comfortable disrobing. Videos filmed on spy-cams hidden in these places have been streamed or uploaded onto public pornography sites. The lack of protections and government response led to massive protests in 2018 in South Korea, where women declared that "my life is not your porn" and demanded increased government action (Bicker 2018).

Another modern-day manifestation of voyeurism is known as "creepshots," where a person takes photos of a woman's body while she is out in public for their personal use or to post publicly for other "creepers" to view and comment on (Thomasen and Dunn, forthcoming 2021). In India, images taken of women's bodies in public have been used to shame and sexualize women online (Gurumurthy, Vasudevan and Chami 2019). A study by Anne Burns on creepshot fora found similar results to those of studies done on non-consensual distribution of intimate images. Users were primarily male; images were mainly of women; commentary consisted of sexually violent, objectifying and racist language about women and their bodies; and there was an aspect of peer bonding or status building within the group (Burns

2018). Burns found that part of the sexual allure of taking and viewing the images was the non-consensual nature of the image, where the person taking the image retains control of the image, rather than the woman featured in it. In a 2018 study, Chrissy Thompson and Mark A. Wood (2018) examined the "storage, classification, curation, and consumption" of creepshots, finding the creepshot website to be a new form of objectifying, classifying and consuming women's bodies that reinforces women's subordination to men. Users of these sites had created "folksonomies of misogyny" that use sexist and racist terms to categorize women as body parts and coached other users to do the same. In some cases, the images are not taken by the voyeur but are copied from the woman's or girl's social media page and then collected together for people to make sexual comments and judge their sexuality, as was the case in the "Top 10" images of Brazil in which preadolescent and adolescent girls' images were categorized from the "prettiest" to the "sluttiest" on social media sites (Valente, Neris and Bulgarelli 2015).

Sexploitation

Anastasia Powell and Nicola Henry (2017, 128) define sexual exploitation, or "sexploitation," as the "commercial exploitation of sex or sexual exploitation material in the media." This would include profiting from websites dedicated to sharing non-consensually distributed intimate images, such as in the case of Hunter Moore mentioned above, as well as other forms of profiting from or purchasing image-based sexual abuse content. In India, the Internet Democracy Project has reported that rape videos have been sold to pornography websites (Srivastava 2017) and are available for purchase in some shops in the country (Masoodi 2016). Mainstream pornography websites have been accused of benefiting from the traffic of users looking for user-generated abusive content. Critics of websites such as PornHub.com and xVideos.com have called on these websites to be more proactive in removing user-generated content of sexual assaults, non-consensually distributed images (Fry 2020) and non-consensual deepfake sexual videos (Burgess 2020). They argue that these companies are profiting from image-based sexual abuse by not removing the content immediately.

Individuals have been commercially exploited through misleading ads for jobs and work contracts. It has been documented in case law in Canada and the United States that women and girls have been tricked into taking sexual images under the guise of a modelling contract, or were told that the sexual images would only be sold for a specific purpose and would not be distributed widely, which was not true (Thomasen and Dunn, forthcoming 2021). In a recent case involving the pornography company GirlsDoPorn.com, it came to light that many of the young women featured in the films had been tricked or coerced into filming their sexual activity by producers who had placed ads for models and later convinced the young women who responded to the ads into filming sexual activity. The models were told that the videos would not be publicly distributed (ibid.). In reality, the videos were featured on popular pornography websites such as PornHub.com and many of the women later had their personal contact information doxed. Following a civil suit against the company, 22 young women were awarded nearly US$13 million in compensatory and punitive damages (*Jane Doe Nos. 1-22 v. GirlsDoPorn.com*).

Sextortion

Sexual extortion, or "sextortion," occurs when an individual has, or claims to have, a sexual image of another person and uses it to coerce a person into doing something they do not want to do (Wittes et al. 2016). By threatening to release the image unless the other person does as they are asked, the person claiming to have the images is able to obtain additional sexual images, unwanted sexual activity, the continuation of a romantic relationship, engagement in human trafficking, money or other things from the victim-survivor (West 2014). Sextortion can happen in the context of a failing romantic relationship but can also be perpetrated by strangers (Powell and Henry 2017). In 2017, a Dutch man named Aydin Coban was convicted of several offences associated with his extortion of dozens of young girls whom he met online. He threatened to, and sometimes did, post their images online or send them to their family members. He had extorted these children over long periods of time and targeted them into sending additional sexual images of themselves. One of these young women was Amanda Todd, a Canadian teen who later died by suicide (Council of Europe 2018). In some instances, the extorter falsely claims that they have a copy of a sexual image, as is the case in sextortion email scams where individuals are blackmailed out of money by someone claiming to have hacked their computer and taken nude photos of them (Netsafe 2020).

LGBTQ+ people are particularly susceptible to sextortion if they are concealing their gender identity or sexual orientation for safety reasons. Threats to out their sexual orientation, gender identity or birth sex can be particularly disturbing for these individuals (Wolak and Finkelhor 2016).

Documenting or Broadcasting Sexual Assault

In cases of documenting or broadcasting sexual assault, the images of the assault are recorded and sometimes disseminated, resulting in an additional form of sexual violence against the victim-survivor (Palmer 2018). The videos can be posted on social media, texted among peers, and sold or traded to people or websites. For example, the Internet Democracy Project has identified a trend in India where people plan rapes or gang rapes to film and then sell copies of the videos at shops (Masoodi 2016). Additional research by Henry and Flynn (2019) has documented the sale and exchange of so-called rape videos online. Their research documented entire websites dedicated to rape pornography and found examples of websites that require users to submit a new authentic rape video in order to gain access to the site, further driving the production of more videos of sexual assault.

Problematically, some perpetrators have not seen the harm in filming sexual assaults (West 2014). Alexa Dodge (2016) has commented on how rape culture is so normalized in North American culture that, in several cases, perpetrators have gleefully filmed and shared their sexual abuse images. After the initial distribution, members of their community openly redistributed and commented on the content via text and on social media, joking about the sexual abuse. Dodge noted that "these photographs, and the resulting bullying and cyberbullying by peers, continue to recreate and extend the trauma of these sexual assaults. In [two of the cases examined by Dodge], the trauma caused by the permanency of these photos and the cyberbullying experienced as a result of their dissemination, in addition to the sexual assault itself," contributed to the targets' deaths by suicide (ibid., 69).

Sexual abuse images can also be broadcast though a livestream. In the last few years, there have been reports of sexual violence and gang rapes being livestreamed to a public audience. In a 2016 case, a teen in the United States was accused of filming her friend's sexual assault and livestreaming it on the video streaming app Periscope, rather than stopping the assault when her friend asked for help (McPhate 2016). In a 2017 incident, someone called the police in Sweden after witnessing three men sexually assaulting a woman on a Facebook livestream that was watched by hundreds of people. It was reported that one of the men stated, "You have been raped" to the woman being assaulted in the video (BBC News 2017). Whether livestreamed or shared in private groups or on public websites, the non-consensual distribution of intimate images has devastating impacts on the target's well-being and sexual autonomy (Henry and Powell 2016).

Synthetic Media

Modern media technology allows for the manipulation of images, making it appear as though people are engaging in sexual activity they never engaged in (Chesney and Citron 2019). Synthetic sexual media has been produced for many reasons, including for sexual entertainment and profit, but they have also been created to harass women and purposely cause them harm (Dunn 2020). Early examples of the misuse of technology to create synthetic sexual images include utilizing Photoshop to superimpose a person's face on the body of a sexual image (Delfino 2019), the practice of which remains fairly common in Bangladesh, India and Pakistan (Sambasivan et al. 2019). The images are often published online with identifying data about the person, such as their phone number (APC 2012). Bytes for All conducted three case studies on women who were targeted by TFGBV in Pakistan. In one case, a human rights activist reported having her image superimposed onto pornographic images, along with receiving hundreds of death and rape threats (Bukhari 2014). In Australia, Noelle Martin discovered that her image had been taken from her social media profile and copied onto multiple pornographic images (Citron 2019). Targeted abuse of her image has occurred over several years and has more recently evolved into people making sexual deepfakes of her (Martin 2017).

As technology has advanced, it is now possible to create realistic-looking sexual images of a person without their consent (Thomasen and Dunn, forthcoming 2021). Employing artificial intelligence, one can swap a person's face onto the face of another person in a sexual deepfake video, making it appear as though they are featured in the sexual video performing sex acts they never participated in (Chesney and Citron 2019). Like other forms of

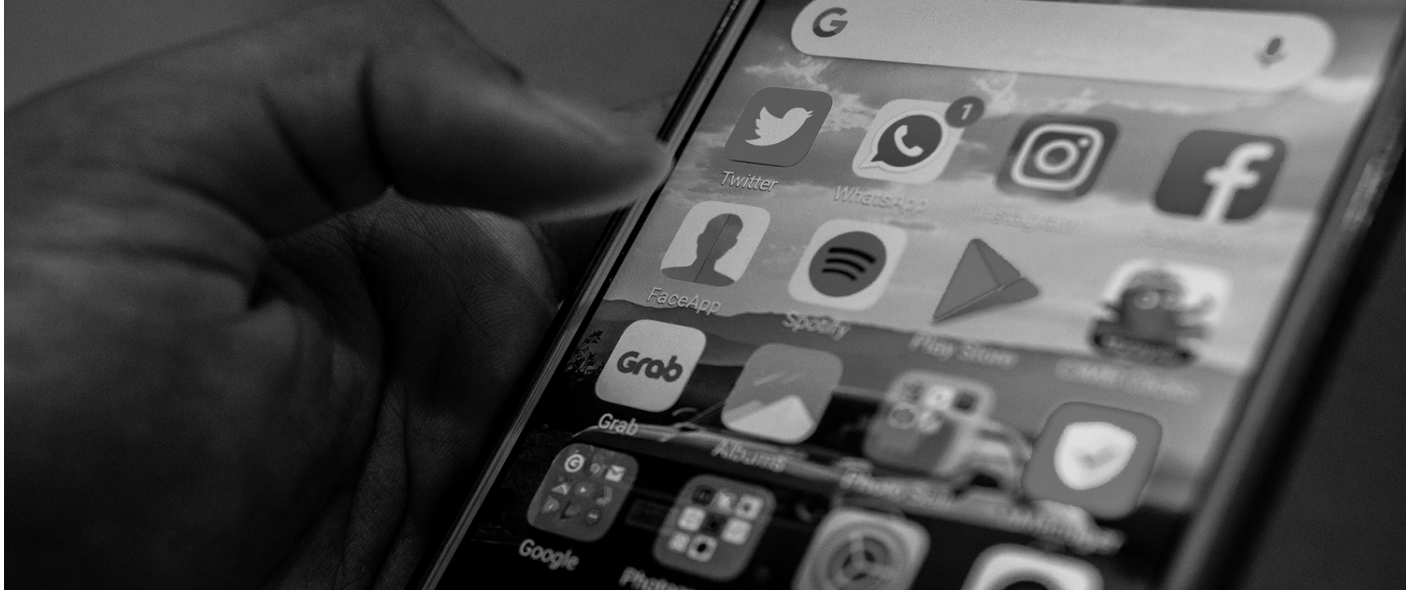

Photo: Aiman Khair/Shutterstock.com

image-based sexual abuse, sexual deepfakes are predominantly made of women. Sensity (formerly Deeptrace) collected data on nearly 15,000 publicly available deepfakes and found that 96 percent of them were sexual deepfakes of women, most of whom did not consent to their images being used (Ajder et al. 2019). Their research showed that deepfake production was not only gendered but also racialized, with a disproportionate amount of deepfake videos being made of South Korean women, compared to non-sexual deepfakes (ibid.). However, it is not only celebrities who are targeted. A journalist in India named Rana Ayyub had a sexual deepfake made of her as part of a networked harassment campaign that targeted her. The harassment against her was so severe that the United Nations released a statement calling on the Indian government to better protect her (UN OHCHR 2018). Danielle Keats Citron has stated that "even though deep-fake sex videos do not depict featured individuals' actual genitals, breasts, buttocks, and anuses, they hijack people's sexual and intimate identities. Much like nonconsensual pornography, deep-fake sex videos exercise dominion over people's sexuality, exhibiting it to others without consent" (Citron 2019, 1921). Similar technology exists that allows users to input a clothed image of a woman to produce a fake nude photo of her without her consent. A recent iteration of this technology has been used more than 100,000 times and only works on women's photos. Unlike deepfakes that primarily target female celebrities, most users of this technology were intending to use images of women they personally knew (Ajder, Patrini and Cavalli 2020). Images created with this technology co-opt women's sexual expression and can also be used to misrepresent and extort the people in the images.

Public Disclosure of Private Information

The publication of private sexual material has clear ramifications for women and girls, but other forms of private information can also cause harms if distributed online. Perpetrators of gender-based violence have published private information about a person in order to harass, embarrass and harm the reputation of their targets (*R. v. Fox*). In communities or families with more conservative or patriarchal values, the publication of private information, such as a screenshot of a woman conversing with a male non-family member or wearing particular clothing, or images of a woman in a particular social situation, can lead to these women being harmed (eSafety Commissioner 2019). Members of the LGBTQ+ community may have good reasons to selectively reveal their sexual orientation. Due to systemic homophobia and trans antagonism (Ashley 2018) and laws that forbid same-sex relationships in certain countries, outing an LGBTQ+ person's sexual orientation or birth sex online can result in significant harms (Younes 2020). The context in which the information is released changes the meaning of personal information, and publication of non-sexual material can be equally, if not more, harmful than the publication of sexual material.

Doxing

One of the more dangerous forms of the publication of private information is doxing. Doxing is the publication of personal information such as a person's legal name, address, phone number, contact information, driver's licence, workplace, and private documents or correspondence without their consent (Thomasen and Dunn, forthcoming 2021). In Sarah Jeong's book *The Internet of Garbage* (2018), she describes the origin of doxing as a

hacking term that means "dropping dox," which involves the publication of documents online. In its current manifestation, doxing has been used to intimidate the victim-survivor by driving online harassment against them and making them fear that they may be harassed or harmed in person.

Many women who speak out about gender inequality or are disliked by misogynistic groups online have been doxed. Amnesty International (2018) found that one-third of all women who experienced online harassment had been doxed. Women who transgress gender norms by appearing anonymously or under a pseudonym in sexual content online have had their real identities exposed in digital spaces. In at least two reported cases, people have used facial recognition software to visually match women in pornography with their social media profiles with the intention of doxing them (Thomasen and Dunn, forthcoming 2021). Once a person's personal information is made public, harassers can then show up at their workplace, threaten them at their home or send harmful messages to their phone, email address or social media accounts. Some people who have been doxed have been forced to change their phone numbers and email addresses and, in more drastic cases, move to new homes and change their legal name (Citron 2014).

Defamation and Misrepresentation

In many countries, the legal definition of defamation includes publishing false information about someone that harms their reputation. In the era of the Google search, a person's reputation can be easily altered if false information is published about them online (Solove 2007). There is a whole industry of companies dedicated to protecting people's reputations online and trying to have defamatory information about a person scrubbed from the internet (Bartow 2009). A study by the Pew Research Center showed that 26 percent of Americans have had something untrue about them posted online (Duggan 2017).

Due to patriarchal gender norms that place restrictions on women's sexuality (Armstrong et al. 2014), a woman's reputation is particularly sensitive to defamatory statements about her sexuality. Online attacks against women and girls often focus on their sexuality and include untrue statements about their sexuality (Bailey 2014, 709).

False content about a person can harm their reputation, but as seen above, the publication of true information or decontextualized private information that misrepresents a person can be harmful as well (Dunn, forthcoming 2021). In many cases, it is a blend of true and false information that actually hurts the person's reputation. In a study conducted for the Law Commission of Ontario, Jane Bailey and Valerie Steeves (2017) interviewed young people about their experiences with online defamation. Participants reported that the lines between true and false information were blurry when it came to content that harmed their reputation, and attackers used both types of information to cause harm. It is this harmful and misrepresentative publication of inappropriate information that can damage a reputation, regardless of its truthfulness.

Stalking and Monitoring

Stalking can be done through the use of technology, such as monitoring a person's social media posts, tracking their location or installing commercial stalkerware on their devices (Lenhart et al. 2016; Khoo, Robertson and Deibert 2019; National Network to End Domestic Violence 2014). It typically involves repeated unwanted monitoring, communication or threatening behaviour that can cause a person to feel fear (Citron 2014). A UK study showed 23.8 percent of stalking victim-survivors said their primary concern about the stalking was fear for their physical safety (Maple, Short and Brown 2011). Women in this study were more likely to fear for their physical safety than men who had been stalked.

Abusive intimate partners are known to stalk their spouses, and reports have shown a difference between genders in relation to stalking. A German study found that women were more likely to be stalked and sexually harassed online, and that the impact was more traumatic for women (Staude-Müller, Hansen and Voss 2012). A report by Statistics Canada (2017) also found women were more likely than men to be stalked online. The European Union Agency for Fundamental Rights (2014) published findings that young women between the ages of 18 and 29 were at particular risk for online stalking. Other surveys have found similar numbers between genders and, in some cases, men were more likely to be targets of stalking online (Henry and Powell 2016).

In intimate partner relationships, it can be quite simple for an abuser to gain access to a partner's whereabouts or private information in order to track them. Karen Levy and Bruce Schneier (2020) have noted that people who live in close proximity to each other, such as romantic partners, family members and friends, may have easy access to another person's device, may share passwords or have ways of discovering them, and may use software that reports the target's location to the other person. Abusers are able to use common apps already stored on their partner's phone, such as the Find My iPhone app, to track their targets. Diana Freed et al. (2017) have described the ways that partners can gain access to accounts through social engineering because they know much of the information needed to connect with a company and gain access to their partner's accounts, or they know the answers to their security questions. The European Union Agency for Fundamental Rights (2014) reported that, in some cases, abusers gave technology to their child so they could use it to gain access to their ex-partner when they had custody of the child.

Advanced technology such as stalkerware, smart home devices and drones have been used to monitor and control women. A 2019 report by Citizen Lab reviewed the use of stalkerware, which is a type of spyware that is installed on a phone or other digital device to keep track of a particular individual (Parsons et al. 2019). Once stalkerware is installed on a device, data is gathered from the device and sent to the person who installed it. This data could include information such as a person's Global Positioning System (GPS) location, copies of their text messages or photos, or copies of everything they have typed into their device, including passwords. In Cambodia, the APC found that abusive men commonly used GPS software and stalkerware to monitor their partners (APC 2012). Smart home technology and home safety systems have also been used to monitor and control women by abusers who maintain access to this technology (Safety Net Canada 2013). Kristen Thomasen's (2018) research has noted that when drones have been used to film women, it negatively affects how women use public spaces. If the technology has recording, listening or tracking capabilities, there is a risk it could be misused by an abuser.

Impersonation

Impersonation can lead to reputational damage and put a person at physical risk. Some abusers have created fake online accounts of women to spread false information and damage the reputation of the person they are impersonating (Gurumurthy, Vasudevan and Chami 2019). Abusers have created fake websites impersonating the victim-survivor in an attempt to ruin their personal relationships and destroy their job prospects (Dunn, forthcoming 2021). They may also send fake messages from the victim-survivor's accounts or fake accounts to damage their personal and professional relationships (Freed et al. 2017). A study from Bangladesh, India and Pakistan found that women who had lower incomes or were younger or sexual minorities were more likely to be impersonated and that the impersonation often had a sexual element (Sambasivan et al. 2019).

Some abusers impersonate someone other than the victim-survivor to glean information about the victim-survivor that they would not normally be able to access (Safety Net Canada 2013). In an example of state-sponsored TFGBV, Egyptian authorities have made fake accounts on social media and LGBTQ+ dating sites, pretending to be members of the LGBTQ+ community in order to locate, arrest and torture lesbians, gay men and transgender women (Human Rights Watch 2020). In highly disturbing cases, vindictive ex-partners have posted fake dating profiles (Citron 2014) or escort ads propositioning men for sex, some going as far as inviting men to women's houses to play out rape fantasies (West 2014). This has led to unwanted visits at the person's workplace and home and, in some cases, has led to violent sexual assaults (APC 2011). In other cases, impersonation has been used to trick women into dangerous situations, including human trafficking, through fake marriage, school or work opportunities (APC 2012).

Threats

Death threats and rape threats have become common and even normalized in online dialogue (Van der Wilk 2018). Research by Safety Net Canada (2013) found that threats and intimidation were the most commonly reported forms of TFGBV against victim services workers in Canada. Women journalists (Barton and Storm 2014; Jane 2018), academics (Veletsianos et al. 2018), politicians and human rights defenders (Amnesty International 2018) face rape threats and death threats online, particularly if they are speaking or writing about equality issues or typically male-dominated topics. Some have received these threats over multiple years and many receive them on a

daily basis. Research commissioned by Amnesty International (ibid.) demonstrated that 41 percent of women who had been harassed on Twitter felt that their physical safety was threatened on at least one occasion of online harassment. The report provided graphic examples of violent rape and death threats sent to women in the study.

Hate Speech

Hate speech is a particularly abhorrent form of TFGBV that dehumanizes and encourages violence toward a person or a group of people based on an identifying feature, such as their religion, gender, ethnicity, disability or other identity factor (Citron 2014). Intersecting identity factors can increase the likelihood that a woman will be targeted by digital hate speech. For example, Muslim women are more likely to be targeted by online hate crimes than Muslim men (Awan and Zempi 2016). Hate speech has proliferated online, with white-supremacist, Islamophobic, anti-Semitic, anti-LGBTQ+ and women-hating groups finding spaces to gather and promote their discriminatory beliefs. Social media platforms have been criticized for profiting from these sites and, in some cases, driving traffic to these sites through their algorithms. In some cases, hateful online rhetoric has led to offline violence. In countries such as India and Sri Lanka, hateful messages about minority groups spread through Facebook, YouTube, Twitter and WhatsApp have led to targeted violence against them (Laub 2019).

Hate speech can target women because of a combination of their identity factors or, more specifically, their gender. In Malawi, 46.3 percent of women surveyed had been subjected to hate speech online (Malanga 2020). Gendered hate speech made up 3.1 percent of reports to internet platforms in the European Union (Van der Wilk 2018). Online hate reinforces systemic inequalities, makes it difficult for certain groups to engage online, and can spill over into the physical world, causing violence and even death. In a case in Pakistan, a woman who had been the target of hate speech was shot at in public due to hate speech aimed at her online (Bukhari 2014).

Social media sites and online chat fora such as 4chan and 8chan have been known to host groups who promote hatred of women (Jane 2014), including incels and MRAs (Ging 2017). In several documented cases, members of these groups have enacted violence against women in the real world. Elliot Rogers, who is hailed as a hero among incels, killed six people after releasing a manifesto online where he stated he was going to get retribution for being rejected sexually by women. Prior to the killings, Rogers posted videos about his hatred of feminists and anger toward women on various sites, including one called sluthate.com. The internet creates spaces for these types of ideas to proliferate (Baele, Brace and Coan 2019). In Canada, there have been two attacks associated with incels: the 2018 Toronto van attack, where a man claiming to be associated with incels ran over multiple people with a rented van (ibid.) and, more recently, the murder of a sex worker by a man claiming to be affiliated with incels (Cecco 2020). These men felt entitled to sex with women and wanted to harm them as retribution for their lack of sexual access to them.

Who Is Affected?

By numbers alone, women and girls are most affected by TFGBV; however, certain groups of people are subjected to this form of violence at higher rates and face qualitatively different kinds of attacks. As with other forms of gender-based violence, women, transgender and gender-nonconforming people across all spectra of race, sexual orientation, ability and class can be targets of TFGBV. This section will review three aspects that increase the risk of being targeted by TFGBV. First, studies have shown that women, transgender and gender-nonconforming people with intersecting inequality factors, such as women of colour, LGBTQ+ women and/or people with disabilities, can face higher levels of online harassment and abuse compared to white, heterosexual, cis-gendered and/or able-bodied women. Second, women in abusive intimate partner relationships are likely to experience TFGBV at the hands of their intimate partners. Third, women in leadership positions, such as politicians, human rights defenders and journalists, experience significantly higher levels of abuse online, particularly if they are speaking about equality issues or on issues traditionally dominated by men.

Intersectional Equality Factors

TFGBV is rooted in racism, misogyny, homophobia, transphobia and other forms of discrimination. Depending on a woman's intersecting identity

factors, she can be targeted by sexist and misogynistic online attacks, as well as attacks that focus on her race, Indigeneity, sexual orientation, disability, religion, gender identity and gender expression (Dhrodia 2018; West 2014; Bailey and Shayan 2016). Intersectionality scholar Patricia Hill Collins (1990) notes that an individual's intersecting social locations cannot be easily separated. How a person experiences sexism will be inherently tied to other aspects of their identity. A Black lesbian experiences sexist online attacks against her not strictly as a woman, but as a Black lesbian woman (Amnesty International 2018). As such, a person's intersecting identity factors will alter the experiences they have online, influencing the qualitative ways they are attacked and the level of violence geared toward them (Dhrodia 2018). For example, racialized women and girls are often subjected to more attacks than white women and girls, and attacks against them focus on their race, whereas race is unlikely to be a factor in online attacks against white women (Amnesty International 2018; Plan International 2020).

In her 2018 international report on online violence against women and girls, the UN Special Rapporteur on violence against women, its causes and consequences found that "young women, women belonging to ethnic minorities and indigenous women, lesbian, bisexual and transgender women, women with disabilities and women from marginalized groups are particularly targeted by ICT [information and communications technology]-facilitated violence" (UN 2018, 8). These amplified inequalities were mirrored in Amnesty International's *Toxic Twitter* study (2018). Amnesty International interviewed 86 women and non-binary people in the United Kingdom and the United States, many of whom were leaders or public figures, and collected quantitative data from hundreds of women from Denmark, Italy, New Zealand, Poland, Spain, Sweden, the United Kingdom and the United States about online violence on Twitter. The study highlighted the intersectional nature of TFGBV, noting that "women of colour, women from ethnic or religious minorities, lesbian, bisexual or transgender women — as well as non-binary individuals — and women with disabilities" (ibid., 7) were at particular risk of harassment on Twitter.

In a global study on gender-based harassment among young women and girls, Plan International (2020) collected qualitative data from 16 countries[5] and quantitative data from 22 countries.[6] More than 14,000 girls and young women participated in the study. Girls who were identified as disabled, Black, LGBTQ+ or politically outspoken online faced worse online harassment than other girls. Many of these girls faced comments that were racist, anti-LGBTQ+ or sexual in nature and that threatened sexual violence. In another study on young women in Southern India, harassment specifically targeted women's caste (four percent) and skin colour (22 percent) (Gurumurthy, Vasudevan and Chami 2019).

The intersectional nature of TFGBV is borne out in research that shows that online abuse aimed at racialized and LGBTQ+ women often combines sexist, racist and homophobic language, and that individuals with intersecting marginalities face higher rates of TFGBV. The US-based Pew Research Center found that online harassment regularly focused on a person's political views, physical appearance, race and gender (Duggan 2017). LGBTQ+ people were particularly targeted with harassment for their sexual orientation. A 2012 study by the European Union Agency for Fundamental Rights (2013) found LGBTQ+ people were harassed and threatened online because of their gender expression and sexual orientation. They were more likely to have their intimate images distributed without their consent. Research by Witness Media Lab (2016) showed that transgender people were attacked in public and that these attacks were filmed and published online along with transphobic commentary. A 2016 study by the Data & Society Research Institute found that lesbian, gay or bisexual American internet users were more likely to have someone threaten to share their sexual images (Lenhart et al. 2016). Brandwatch and Ditch the Label (2019) analyzed 10 million online posts in the United States and the United Kingdom over a three-and-a-half-year period, locating 1.5 million transphobic comments. Common themes among these abusive comments targeting transgender people included racist and gender-based comments.

5 Canada, Chile, Ecuador, El Salvador, Guinea, Indonesia, Malawi, Myanmar, Nepal, Peru, the Philippines, South Sudan, Spain, Sudan, Tanzania and the United States.

6 Australia, Benin, Brazil, Canada, Colombia, Dominican Republic, Ecuador, Germany, Ghana, Guinea, India, Indonesia, Japan, Kenya, the Netherlands, Nigeria, Norway, the Philippines, Spain, Thailand, the United States and Zambia.

Race and gender were common intersecting identity factors that resulted in increased abusive harassment online. Lisa Nakamura (2013) has documented rampant sexism, racism and homophobia within the online gaming community, where discriminatory comments often combined racist, homophobic and sexist terms. A 2017 Pew Research Center study in the United States found that people of colour, especially Black people, were targeted online because of their race. Twenty-five percent of Black adults had been harassed because of their race or ethnicity (Duggan 2017). Amnesty International (2018) examined abusive tweets aimed at members of Parliament (MPs) in the United Kingdom over a particular time period and found that Diane Abbott, the only Black female MP, had received nearly half of all abusive tweets aimed at women MPs.

Intimate Partner Violence

Women who are in abusive intimate partner relationships are one of the most common targets of TFGBV (Laxton 2014). In a 2015 study, the APC found that two-thirds of all online abuse was conducted by a current or previous intimate partner (APC 2015). Studies conducted in Norway (Hellevik and Øverlien 2016), Spain (Borrajo et al. 2015) and the United States (Burke et al. 2011) found significant numbers of young people reported experiencing TFGBV in intimate partner relationships. These abusive intimate partners have used technology to stalk and monitor their partners and ex-partners (Freed et al. 2017), send insulting and threatening messages via text or social media sites, disclose humiliating private information about their partner online, and monitor their partner's devices and social media accounts (Borrajo et al. 2015). This behaviour causes women to feel fearful and as though their partner is always watching them (Woodlock 2015).

Unlike strangers, intimate partners may have access to their target's devices and accounts. They may know the passwords to these accounts and have all of their partners' contact information, allowing for surveillance and harassment (Levy and Schneier 2020). Technology serves as a convenient tool to maintain violent control over a partner. Several organizations working with victims of domestic violence have conducted studies on the use of technology to abuse women. A 2015 SmartSafe study from Australia found that 98 percent of victim services workers had encountered clients who had experienced TFGBV in their intimate relationships (Woodlock 2015). Women's Aid, a British organization, found that 45 percent of women who had been abused in intimate partner relationships had been abused via technology during the relationship, and 48 percent experienced TFGBV after the relationship ended (Laxton 2014). Online abuse can be part of a pattern of physical intimate partner violence; the provincial domestic violence review committee in Ontario, Canada, found that TFGBV was a theme in many of the fatality cases they examined in 2010 (Office of the Chief Coroner 2011). This increasing prevalence of TFGBV is a serious concern for women and girls who already are disproportionately suffering in violent intimate partner relationships, particularly because TFGBV is often minimized as an insignificant form of abuse (West 2014).

Women in Leadership Roles

Women are under-represented in leadership roles worldwide. There is a critical need for greater gender diversity in politics, journalism and other leadership positions; however, this need is stifled when women leaders experience harassment online. Unfortunately, women leaders face unique and burdensome forms of TFGBV that challenge their ability to continue their work. Online attacks against women in leadership roles cause harms to the women targeted, but they also have the systemic effect of keeping women out of leadership roles because they fear being attacked online. Girls and young women begin facing this type of abuse at a young age when they act as vocal leaders. Plan International's (2020) global study on girls' and young women's experiences with online harassment found that girls who spoke about political issues such as race, feminism and human rights faced higher rates of harassment online compared to girls and young women who did not speak out about political issues.

International human rights bodies have recognized this troubling trend and have called for change. The 2018 report on TFGBV by the Special Rapporteur on violence against women, its causes and consequences found that "some groups of women, such as women human rights defenders, women in politics, including parliamentarians, journalists, bloggers…are particularly targeted by ICT-facilitated violence" (UN 2018, 8). Recognizing the harms of this violence, the UN Special Rapporteurs on violence against women, its causes and consequences, and

on the promotion and protection of freedom of opinion and expression noted that TFGBV chills the speech of "women journalists, activists, human rights defenders, artists and other public figures and private persons," limiting women's ability to participate in all areas of life (UN OHCHR 2017).

For some female journalists, receiving digital harassment and violent threats has become a regular occurrence in their profession; they are insulted and threatened on social media, via email and in the comment sections of their articles (Barton and Storm 2014; Reporters Without Borders 2018). Research by the International Women's Media Foundation found that "physical, sexual and online abuse is a part of women journalists' daily work" (Ferrier 2018, 7). Global Information Society Watch reported that women bloggers, journalists and leaders were disproportionately subjected to online abuse and violent sexual attacks, especially if they were in sectors that had traditionally been male-dominated (Finlay 2013). In Latin American countries, where physical violence is directly linked to online harassment, these threats are very serious. Online threats of sexual violence, "corrective rape," and kidnapping against journalists and activists can materialize in real life, and it can be difficult to differentiate between misogynistic abusers trying to cause emotional distress and those who actually follow through with their threats (Ruiz-Navarro 2016).

This violence stifles the voices of women and issues that are important to them. Almost two-thirds of women journalists surveyed by Global Information Society Watch had been threatened or harassed and around 40 percent had avoided reporting on certain topics because of this harassment (Finlay 2013). According to the Organization for Security and Co-operation in Europe (2016), female journalists are being "coerced into silence" because of the sheer volume of death threats, rape threats, threats of physical violence and graphic imagery they receive.

While women writing on topics related to inequality and human rights were specifically targeted, women journalists face higher volumes of attacks regardless of the topic they are writing on. Research on comments made on *The Guardian* website found that the contributing women journalists were harassed at significantly higher rates in comparison to their male colleagues: "Articles written by women attract more abuse and dismissive trolling than those written by men, regardless of what the article is about" (*The Guardian* 2016).

State-sponsored attacks on women journalists have been reported in several countries, including Brazil. In 2020, Bianca Santana reported to the forty-fourth session of the United Nations Human Rights Council how she and other women journalists had been attacked by Brazilian President Jair Bolsonaro after writing critical pieces about the government, including through online harassment and smear campaigns (Article 19 2020). The International Center for Journalists and the United Nations Educational, Scientific and Cultural Organization are currently conducting a global survey on TFGBV against women journalists, and their initial research highlights state- and/or public-based harassment against journalists in India, Malta, the Philippines and the United Kingdom (Posetti 2020).

Female bloggers and human rights defenders are subjected to attacks similar to those faced by journalists, especially if they are writing on issues related to gender equality (Eckert 2018). Feminists are specifically (Sundén and Paasonen 2018) and disproportionately (Lewis, Rowe and Wiper 2016) targeted online by trolls and abusive internet users. Amnesty International (2018) found that when women were talking about issues such as reproductive rights or anti-Black racism online, the harassment against them only increased. A survey by the APC (2017) on sexual and reproductive activists found that 64 percent of cis-women activists received threatening and intimidating comments online related to their advocacy. The same organization conducted multiple studies on sexual rights activists in Brazil, India, Indonesia, Lebanon, Nepal, South Africa, Sri Lanka, Turkey and the United States, finding both state and non-state actors curtailed the activists' advocacy and policed their sexuality online (Valle 2020). Many face offline attacks and even problematic state responses. In Saudi Arabia, a women's rights activist was arrested for being in public without a hijab after she tweeted that she was going out without an abaya and to smoke a cigarette (Thorsen and Sreedharan 2019).

Women politicians are also at particular risk. As a part of their job, women politicians use social media platforms to engage with their constituents, share information and hear from the general public. If they become fearful of engaging online because of the violence they face, this impacts their ability to serve their constituents and be effective politicians (Dhrodia 2018). An Inter-Parliamentary Union (2016)

study on sexism, sexual harassment and violence against women parliamentarians from African, Arabic, Asia-Pacific, North and South American, and European countries showed 81.8 percent had been harassed, and 44.4 percent had received threats of "death, rape, beatings or abduction during their parliamentary term." They faced discriminatory comments about their gender, experienced sexual harassment, and were delegitimized through sexist comments about their clothing and manner of speaking. Social media platforms were common sites of this abuse. The study expressed concern about the longer-term impact of this harassment, in that it would discourage women from participating in politics. In the current online environment where death and rape threats are ever-present, women journalists, bloggers, human rights defenders and politicians have to make the difficult choice between continuing to advocate for equality online and face abusive online harassment, or to be silent.

What Are the Harms?

The harms caused by TFGBV are felt both at the individual and the systemic level (Bailey and Mathen 2019). Individual people can have their privacy invaded and their autonomy threatened, experience psychological harms, feel fearful, limit their expression and face reputational, professional and economic consequences. Yet, on a broader scale, this violence also has significant systemic impacts. It reinforces inequality and maintains discriminatory norms that limit women and transgender people from living with freedom and realizing all of their human rights. It maintains and reinforces patriarchal gender hierarchies and institutionally undermines the violence experienced by those targeted by TFGBV. Researchers in lower- and middle-income countries have been particularly robust in their analysis of the intersectional, political, institutional and structural linkages associated with TFGBV, recognizing how institutional power, social hierarchies and the digital divide each play a role in contributing to TFGBV. This section will review some of the more commonly reported harms in research to date, including psychological and emotional harms, privacy invasions, risks to safety, the silencing of women's voices and economic damages.

Psychological and Emotional Harms

TFGBV can take a serious mental toll on victim-survivors. This form of violence can be relentless and widespread, leaving no avenue for escape because the victim-survivor is always accessible through social media, text or their digital devices. Some live in constant fear of their abusers, others are exhausted from managing the abuse, while others suffer severe mental health impacts such as post-traumatic stress disorder (PTSD) and suicidal ideation, or a combination of all of these psychological and emotional harms (Henry and Powell 2016). Sixty-five percent of the women surveyed by Battered Women's Support Services in Vancouver, British Columbia, reported psychological impacts of TFGBV ranging from anxiety and damaged self-esteem to suicidal ideation (West 2014). In Southern India, 28 percent of the 326 women surveyed felt anxious or depressed as a result of the violence and six percent reported attempting to self-harm (Gurumurthy, Vasudevan and Chami 2019).

According to the Pew Research Center, those who have experienced more severe forms of online harassment, such as threats, stalking, sexual harassment and harassment over a long time period, are more likely to experience negative impacts on their relationships offline and suffer from mental distress (Duggan 2017). Research by the Women's Legal and Human Rights Bureau, Inc. (2015) found that women targeted by TFGBV in Bosnia, Democratic Republic of the Congo, Kenya and Mexico faced a variety of mental health harms, including stress, anxiety and depression. Fifty-three percent of women surveyed in Senegal suffered from mental stress and anxiety following online attacks (Iyer, Nyamwire and Nabulega 2020). For the young women and girls surveyed by Plan International (2020), emotional distress, anxiety and depression were the second most common effect of TFGBV.

Specific forms of TFGBV have been known to cause serious mental health outcomes. Qualitative data collected by Samantha Bates (2016) found that women who had their intimate images shared without their consent experienced similar forms of psychological distress as those who had been sexually assaulted. They reported experiencing issues with trust, anxiety, depression, PTSD, suicidal ideation and other mental health

impacts. A study by the University of Bedfordshire concerning online stalking found that technology-facilitated stalking can cause PTSD in the victim-survivor (Maple, Short and Brown 2011).

The emotional and psychological stressors caused by TFGBV have tangible real-world impacts on women. The psychological impact of online harassment makes it difficult for women to focus on school and work. Women polled by Amnesty International (Dhrodia 2018) found that more than half (56 percent) of the women who were harassed on Twitter struggled to focus on everyday tasks and felt stress, anxiety or panic attacks (55 percent) after experiencing harassment or abuse. The psychological and emotional effects of TFGBV can cause targets to alter their behaviour, conforming to patriarchal gender norms in order to avoid additional violence (Gurumurthy, Vasudevan and Chami 2019).

Privacy

Several forms of TFGBV involve invasions of privacy. Whether these forms include hacking into a woman's digital device or online accounts, installing spyware on her phone, secretly filming her for a sexual purpose or sharing her private information online in hurtful ways, privacy invasions are a central component of TFGBV. Marginalized groups including women, LGBTQ+ people, Black people, Indigenous people and people of colour have not traditionally been fully protected by privacy norms and are at risk of privacy invasions specific to their identities, such as the non-consensual publication of women's intimate images, race-based police targeting or the unwanted outing of LGBTQ+ people's identities (Thomasen and Dunn, forthcoming 2021). When women are fearful about their private information being stolen or released by abusive people, it limits their ability to express themselves in digital spaces or save private content via digital means. In Palestine, women reported family members and governments using technology to monitor their behaviour, leading to self-censorship and limited information sharing. Only 39.8 percent of Palestinian women felt safe posting personal information on social media, with 50 percent refusing to share any photos online, and many feared being exposed without their hijab online (Arab Center for Social Media Advancement 2018).

Privacy invasions can bring unwanted attention to someone and expose them to ongoing harassment following the release of private information about them. Once personal information is released online, it can be difficult, if not impossible, to get back (McGlynn and Rackley 2017). It may remain permanently on the internet or stored on another person's device, maintaining the risk of future privacy invasions (Citron 2014). This can impact a person's autonomy. For example, women who are being stalked and monitored online lose their freedom of movement; they cannot move about the world without fear of surveillance (Parsons et al. 2019). Danielle Keats Citron (2019) has written about how the publication of private sexual images affects a woman's bodily integrity and ability to choose how she expresses herself sexually. Invasions of privacy can make a person feel monitored, put their safety at risk, limit their freedom of expression and impact their ability to define their personhood.

Safety

Many victim-survivors have legitimate reasons to fear for their psychological and physical safety when they experience TFGBV. The offline world is not separate from the online world, and victim-survivors face real-world impacts when they are targeted by TFGBV (Van der Wilk 2018). Stalkers do not always limit their stalking to digital spaces; abusive partners use digital and physical tactics to torment their victims, and some cases of impersonation have led to brutal physical rapes. Further, online threats have resulted in physical violence and/or a perceived sense of impending violence, causing targets to change their offline behaviour out of fear (Angus Reid 2016).

In Malawi, 53.7 percent of women surveyed experienced physical abuse exacerbated by online violence (Malanga 2020). A Canadian study by Angus Reid (2016) found that women were much more likely to have their social media harassment follow them into the real world. Feminist advocates such as Anita Sarkeesian have been viciously attacked online, requiring them to hire additional security for their events and causing them to fear presenting their work in public due to certain threats (Citron 2014). The Pew Research Center found that one in 10 people who had been harassed online felt a risk to their physical safety or the safety of people close to them (Duggan 2017). In a study by the Battered Women's Support Services, five percent of the women surveyed were physically harmed as a result of TFGBV (West 2014). Twenty-nine percent

of women who experienced online harassment in Southern India felt continually afraid for their safety (Gurumurthy, Vasudevan and Chami 2019). This risk to safety creates societal burdens on those targeted who may experience physical harms but will also be limited in their freedom of movement.

Silencing

TFGBV silences the voices of women online, causing them to self-censor and reduce or end their participation in digital spaces and leadership roles (Amnesty International 2018; Plan International 2020). The systemic impact of this silencing reinforces patriarchal gender roles, discourages women from taking up leadership roles, and reduces online content related to equality and human rights. In Ethiopia, Kenya, Senegal, South Africa and Uganda, women reported that the more they spoke up online, the more violence they experienced, forcing them to make the difficult choice between expression and safety (Iyer, Nyamwire and Nabulega 2020). In an Indian study, young Muslim Indian women adopted self-regulating practices such as deleting any content that would make them appear sexual out of fear of repercussions (Mishra and Basu 2014). Women's voices and contributions are targeted both for their personal content and for broader expression online. For example, Wikipedia has a large gender gap, with less than 10 percent of its contributors being female (Wikimedia 2018). This lack of female contributors, and the lack of content on women and women's issues, is reportedly due to the hostility many women editors face from their male colleagues (Eckert and Steiner 2013; Paling 2015).

Multiple studies show that victim-survivors of TFGBV reduce their time online or alter what they post online in order to avoid this type of abuse. Battered Women's Support Services found that the most common response to TFGBV by victim-survivors was to limit their online comments (West 2014). A study on cybercrimes in India found that 28 percent of women intentionally reduced their online presence after being harassed online (Pasricha 2016), whereas another study from Southern India found that 57 percent of women who were harassed online were cautious about posting content on their social media (Gurumurthy, Vasudevan and Chami 2019). In Malawi, close to 70 percent of the women surveyed withdrew from online activity because of TFGBV (Malanga 2020). Amnesty International (2018) reported that when women are harassed online, they self-censor, alter the content of their online posts and sometimes leave social media spaces entirely. The organization also found that between 63 percent and 83 percent of women who had been harassed online changed the way they used social media, and 32 percent said they stopped posting content about certain issues that are important to them. Similar results were found by Battered Women's Support Services: 40 percent of women withdrew from online activity after experiencing TFGBV, and 15 percent left social media platforms altogether (West 2014). Women and girls are learning this lesson of being silenced online from an early age. In a study of young women and girls across 16 countries, 47 percent of those who spoke out politically online faced attacks about their opinions (Plan International 2020).

TFGBV has become so pervasive that some victim-survivors begin to normalize or tolerate it. Research on academic women who had been harassed online (Veletsianos et al. 2018) shows that they minimize the violence and sometimes blame themselves for the abuse they receive online. Plan International (2020) found that many of the young women and girls it surveyed normalized TFGBV; they were more likely to ignore the violence than resist it as they got older, in part, because they learned to deal with abusers, finding it "not a big deal" or getting "used to it" (ibid., 28). These reports are troubling. They show how TFGBV prevents women and girls from participating in online communication, stifles conversations and advocacy about equality, and dissuades women from taking up leadership positions. Women, transgender and gender-nonconforming people should be free to participate in digital spaces without fear of violence.

Economic Harms

Economic harms can be caused intentionally or unintentionally by the abuser. Certain abusers act deliberately and state openly that their intention is to harm their target financially, such as by trying to make them lose their jobs or become unemployable, whereas in other cases, the economic impacts are secondary to the violence (Jane 2018). Online harassment has led to problems at work, problems at school and financial losses, and has made it difficult for some people to find a job due to the reputational damage caused by the abuse and increased stressors impacting work productivity (Citron 2014; Angus Reid 2016). In a report from Malawi, 76.1 percent of women who

experienced TFGBV had some form of associated loss of income and 12 percent were unable to find new employment opportunities (Malanga 2020). In cases involving the non-consensual distribution of intimate images, women have been fired or expelled from school when their intimate images were shared without their consent (Goldberg 2019).

Even if the intention of the abuser is not to economically harm their target, managing TFGBV takes a great deal of emotional labour (Veletsianos et al. 2018) and comes with additional financial costs. It can result in significant costs in mental health supports, legal fees (Citron 2014) or fees to online content management companies (Bartow 2009). For women whose work requires them to engage online, they may lose contracts, paid work or opportunities when they reduce their online presence in order to protect themselves from TFGBV (Amnesty International 2018). Some women have had to replace their technical devices, change their phone numbers (Freed et al. 2017) or move to different homes. A study by the European Union Agency for Fundamental Rights (2014) found that of the women who had been stalked, 23 percent had to change their phone number or email address because of the most serious incident of stalking they experienced. Even women's credit ratings can be affected. Battered Women's Support Services found that 13 percent of victim-survivors of TFGBV experienced job impacts and 10 percent experienced damage to their credit rating (West 2014). TFGBV can have serious financial implications and has proven to be more expensive than more traditional forms of gender-based violence (YWCA 2017).

Conclusion

Research to date demonstrates that TFGBV is a growing international problem that needs additional study, particularly across regions in lower- and middle-income countries in the Global South. This introductory paper serves as a preliminary overview of some of the research that has been done internationally, with a particular focus on three aspects of TFGBV. First, it identified several of the more common forms of TFGBV, including harassment, image-based sexual abuse, public disclosure of private information, defamation and misrepresentation, stalking and monitoring, impersonation, threats and hate speech. Second, it looked at groups of people who face higher rates of TFGBV, including women, girls and transgender, non-binary and gender-nonconforming people with intersecting inequality factors such as race, disability, sexual orientation, caste and gender expression; victim-survivors of intimate partner violence; and women in leadership roles such as politicians, journalists and advocates. Third, it reviewed some of the more common harms of TFGBV, including psychological/emotional harms, privacy violations, safety risks, speech harms and economic damages. This research revealed that although there is a growing body of studies on TFGBV, there is still a pressing need for additional research, specifically empirical research and research centred on the Global South.

Following this introductory paper, CIGI and the IDRC will embark on additional research to contribute to this growing research area. The Supporting a Safer Internet: Global Survey of Gender-Based Violence Online project will survey victim-survivors of TFGBV across the world. It will map the prevalence of TFGBV in 18 countries: Algeria, Argentina, Brazil, Canada, Chile, China, Colombia, Ecuador, France, Germany, India, Jordan, Kenya, Saudi Arabia, South Africa, Tunisia, United Arab Emirates and the United States. In this study, a CIGI-Ipsos survey will collect data on the forms of TFGBV and its impacts on participants in the study. Along with regional experts on TFGBV, CIGI and the IDRC will use this data to produce additional reports that will analyze how this problem manifests itself regionally and to provide cross-jurisdictional comparisons. This research will provide opportunities for policy makers, advocates and educators to learn more about TFGBV and its manifestations worldwide. However, this work will be predominantly focused on the experiences of people in lower- and middle-income countries, where the least amount of research exists to date. This focus will enrich the global understanding of TFGBV.

Works Cited

African Development Bank Group. 2016. "Training of law enforcers to stem rising gender-based cyber violence kicks off in Kenya." African Development Bank Group, April 28. www.afdb.org/en/news-and-events/training-of-law-enforcers-to-stem-rising-gender-based-cyber-violence-kicks-off-in-kenya-15629.

Aikenhead, Moira. 2018. "Non-Consensual Disclosure of Intimate Images as a Crime of Gender-Based Violence." *Canadian Journal of Women and the Law* 30 (1): 117–43.

Ajder, Henry, Giorgio Patrini and Francesco Cavalli. 2020. *Automating Image Abuse: Deepfake Bots on Telegram.* Sensity. www.medianama.com/wp-content/uploads/Sensity-AutomatingImageAbuse.pdf.

Ajder, Henry, Giorgio Patrini, Francesco Cavalli and Laurence Cullen. 2019. *The State of Deepfakes: Landscape, Threats, and Impact.* Deeptrace. https://regmedia.co.uk/2019/10/08/deepfake_report.pdf.

Amnesty International. 2018. *Toxic Twitter.* Amnesty International. www.amnesty.org/en/latest/research/2018/03/online-violence-against-women-chapter-1/.

Angus Reid. 2016. "Trolls and tribulations: One-in-four Canadians say they're being harassed on social media." Angus Reid, October 21. http://angusreid.org/social-media/.

APC. 2011. "Map it. End it. Take Back the Tech!" APC, November 11. www.apc.org/en/news/map-it-end-it-take-back-tech.

———. 2012. "Voices from digital spaces: Technology-related violence against women." APC, April 19. www.apc.org/en/node/14236/.

———. 2015. "Technology-Related Violence Against Women — a briefing paper." APC Women's Rights Programme, Briefing Paper on Violence Against Women. www.apc.org/sites/default/files/HRC%2029%20VAW%20a%20briefing%20paper_FINAL_June%202015.pdf.

———. 2017. *EROTICS Global Survey 2017.* APC. www.apc.org/sites/default/files/Erotics_2_FIND-2.pdf.

Arab Center for Social Media Advancement. 2018. "Online GBV in Palestine Means Losing Out on Women's Participation." Arab Center for Social Media Advancement, June 11. www.genderit.org/feminist-talk/online-gbv-palestine-means-losing-out-womens-participation.

Armstrong, Elizabeth A., Laura T. Hamilton, Elizabeth M. Armstrong and Jessica Lotus Seeley. 2014. "'Good Girls': Gender, Social Class, and Slut Discourse on Campus." *Social Psychology Quarterly* 77 (2): 100–22.

Article 19. 2020. "HRC44: Organisations denounce Bolsonaro government attacks on women journalists." Article 19, July 10. www.article19.org/resources/hrc44-organisations-denounce-bolsonaro-government-attacks-on-women-journalists/.

Ashley, Florence. 2018. "Genderfucking Non-Disclosure: Sexual Fraud, Transgender Bodies, and Messy Identities." *Dalhousie Law Journal* 41 (2): 339–77.

Awan, Imran and Irene Zempi. 2016. "The affinity between online and offline anti-Muslim hate crime: Dynamics and impacts." *Aggression and Violent Behavior* 27: 1–8.

Backhouse, Constance. 2012. "Sexual Harassment: A Feminist Phrase that Transformed the Workplace." *Canadian Journal of Women and the Law* 24 (2): 275–300.

Backhouse, Constance, Donald McRae and Nitya Iyer. 2015. *Report of the Task Force on Misogyny, Sexism and Homophobia in Dalhousie University Faculty of Dentistry.* Halifax, NS: Dalhousie University.

Baele, Stephane J., Lewys Brace and Travis G. Coan. 2019. "From 'Incel' to 'Saint': Analyzing the violent worldview behind the 2018 Toronto attack." *Terrorism and Political Violence* 1–25.

Bailey, Jane. 2014. "'Sexualized Online Bullying' Through an Equality Lens: Missed Opportunity in *AB v. Bragg*?" *McGill Law Journal* 59 (3): 709–37.

———. 2020. "Implicitly Feminist? The Supreme Court of Canada's Decision in *R v Jarvis.*" *Canadian Journal of Women and the Law* 32 (1): 196–220.

Bailey, Jane and Carissima Mathen. 2019. "Technology-facilitated violence against women & girls: Assessing the Canadian criminal law response." *Canadian Bar Review* 97 (3): 664–96.

Bailey, Jane and Sara Shayan. 2016. "Missing and Murdered Indigenous Women Crisis: Technological Dimensions." *Canadian Journal of Women and the Law* 28 (2): 321–41.

Bailey, Jane and Valerie Steeves. 2017. *Defamation Law in the Age of the Internet: Young People's Perspectives.* Commissioned by the Law Commission of Ontario. www.lco-cdo.org/wp-content/uploads/2017/07/DIA-Commissioned-Paper-eQuality.pdf.

Barton, Alana and Hannah Storm. 2014. *Violence and Harassment against Women in the News Media: A Global Picture.* Washington, DC: International Women's Media Foundation and London, UK: International News Safety Institute.

Bartow, Ann. 2009. "Internet Defamation as Profit Center: The Monetization of Online Harassment." *Harvard Journal of Law and Gender* 32 (2): 383–429.

Bates, Samantha. 2016. "Revenge Porn and Mental Health: A Qualitative Analysis of the Mental Health Effects of Revenge Porn on Female Survivors." *Feminist Criminology* 12 (1): 22–42.

Baum, Katrina, Shannan Catalano, Michael Rand and Kristina Rose. 2012. "Stalking Victimization in the United States." Bureau of Justice Statistics Special Report NCJ 224527. www.justice.gov/sites/default/files/ovw/legacy/2012/08/15/bjs-stalking-rpt.pdf.

BBC News. 2017. "Facebook Live 'broadcasts gang rape' of woman in Sweden." BBC News, January 23. www.bbc.com/news/world-europe-38717186.

Bicker, Laura. 2018. "South Korea's spy cam porn epidemic." BBC News, August 2. www.bbc.com/news/world-asia-45040968.

Borden, Diane L. 1997. "Patterns of harm: An analysis of gender and defamation." *Communication Law and Policy* 2: 105–41.

Borrajo, Erika, Manual Gámez-Gaudix, Noemí Pereda and Esther Calvete. 2015. "The Development and Validation of the Cyber Dating Abuse Questionnaire among Young Couples." *Computers in Human Behavior* 48: 358–65.

Brandwatch and Ditch the Label. 2019. *Exposed: The Scale of Transphobia Online*. Brandwatch and Ditch the Label. www.brandwatch.com/reports/transphobia/.

Bukhari, Gul. 2014. *Technology Driven Violence Against Women*. Islamabad, Pakistan: Bytes for All. https://bytesforall.pk/publication/technology-driven-violence-against-women.

Burgess, Matt. 2020. "Deepfake porn is now mainstream. And major sites are cashing in." *Wired*, August 22. www.wired.co.uk/article/deepfake-porn-websites-videos-law.

Burke, Sloane C., Michele Wallen, Karen Vail-Smith and David Knox. 2011. "Using technology to control intimate partners: An exploratory study of college undergraduates." *Computers in Human Behavior* 27 (3): 1162–67.

Burns, Anne. 2018. "Creepshots and Power: Covert Sexualised Photography, Online Communities and the Maintenance of Gender Inequality." In *The Evolution of the Image: Political Action and the Digital Self*, edited by Marco Bohr and Basia Sliwinska, 27–40. New York, NY: Routledge.

Cecco, Leyland. 2020. "Canada police say machete killing was 'incel' terror attack." *The Guardian*, May 19. www.theguardian com/world/2020/may/19/toronto-attack-incel-terrorism-canada-police.

Chesney, Robert and Danielle Keats Citron. 2019. "Deep Fakes: A Looming Challenge for Privacy, Democracy, and National Security." *California Law Review* 107: 1753–1819.

Chisala-Tempelhoff, Sarai and Monica Twesiime Kirya. 2016. "Gender, law and revenge porn in Sub-Saharan Africa: a review of Malawi and Uganda." *Palgrave Communications* 2: 1–9.

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

———. 2019. "Sexual Privacy." *Yale Law Journal* 128 (7): 1870–1960.

Collins, Patricia Hill. 1990. *Black Feminist Thought: Knowledge, Consciousness, and the Politics of Empowerment*. London, UK: Routledge.

Copel, Linda Carman. 2006. "Partner Abuse in Physically Disabled Women: A Proposed Model for Understanding Intimate Partner Violence." *Perspectives in Psychiatric Care* 42 (2): 114–29.

Council of Europe. 2018. *Mapping study on cyberviolence*. T-CY(2017)10. July 9. Strasbourg, France: Council of Europe. https://rm.coe.int/t-cy-2017-10-cbg-study-provisional/16808c4914.

DeKeseredy, Walter S. and Martin D. Schwartz. 2016. "Thinking Sociologically About Image-Based Sexual Abuse: The Contribution of Male Peer Support Theory." *Sexualization, Media, & Society* 2 (4): 1–8.

Delfino, Rebecca A. 2019. "Pornographic Deepfakes: The Case for Federal Criminalization of Revenge Porn's Next Tragic Act." *Fordham Law Review* 88 (3): 887–938.

Dhrodia, Azmina. 2018. "Unsocial Media: A Toxic Place for Women." *IPPR Progressive Review* 24 (4): 380–87.

Digital Rights Foundation. 2018. *Cyber Harassment One Year Report, December 2017 – November 2018*. Lahore, Pakistan: Digital Rights Foundation.

Dodge, Alexa. 2016. "Digitizing rape culture: Online sexual violence and the power of the digital photograph." *Crime, Media, Culture: An International Journal* 12 (1): 65–82.

Dragiewicz, Molly, Jean Burgess, Ariadna Matamoros-Fernández, Michael Salter, Nicolas P. Suzor, Delanie Woodlock and Bridget Harris. 2018. "Technology facilitated coercive control: Domestic violence and the competing roles of digital media platforms." *Feminist Media Studies* 18 (4): 609–25.

Driscoll, Kent. 2020. "Targeted: Inuit women face harassment — online and off." APTN National News, February 20. www.aptnnews.ca/national-news/targeted-inuit-women-face-harassment-online-and-off/.

Duggan, Maeve. 2014. "5 facts about online harassment." Pew Research Center, October 30. www.pewresearch.org/fact-tank/2014/10/30/5-facts-about-online-harassment/.

———. 2017. "Online Harassment 2017." Pew Research Center, July 11. www.pewresearch.org/internet/2017/07/11/online-harassment-2017/.

Dunn, Suzanne, Julie S. Lalonde and Jane Bailey. 2017. "Terms of Silence: Weaknesses in Corporate and Law Enforcement Responses to Cyberviolence against Girls." *Girlhood Studies* 10 (2): 80–96.

Dunn, Suzie. 2020. "Identity Manipulation: Responding to Advances in Artificial Intelligence and Robotics." Paper delivered at We Robot 2020, Ottawa, May 27.

———. Forthcoming 2021. "Is It Actually Violence? Framing Technology-Facilitated Abuse as Violence." In *The Emerald International Handbook of Technology-Facilitated Violence and Abuse,* edited by Asher Flynn, Nicola Henry and Jane Bailey. Bingley, UK: Emerald Publishing Ltd.

Dunn, Suzie and Alessia Petricone-Westwood. 2018. "More than 'revenge porn': Civil remedies for the non-consensual distribution of intimate images." Presentation delivered at the 38th Annual Civil Litigation Conference, Montebello, QC, November 16–17.

Eckert, Stine. 2018. "Fighting for recognition: Online abuse of women bloggers in Germany, Switzerland, the United Kingdom, and the United States." *New Media & Society* 20 (4): 1282–1302.

Eckert, Stine and Linda Steiner. 2013. "Wikipedia's Gender Gap." In *Media Disparity: A Gender Battleground,* edited by Cory L. Armstrong, 87–98. Lanham, MD: Lexington Books.

Elmer, Greg, Anthony Glyn Burton and Stephen J. Neville. 2020. "Zoom-bombings disrupt online events with racist and misogynist attacks." *The Conversation,* June 9. https://theconversation.com/zoom-bombings-disrupt-online-events-with-racist-and-misogynist-attacks-138389.

eSafety Commissioner. 2019. *eSafety for Women from Culturally and Linguistically Diverse Backgrounds.* Summary report, February. www.esafety.gov.au/sites/default/files/2019-07/summary-report-for-women-from-cald-backgrounds.pdf.

European Institute for Gender Equality. 2017. *Cyber violence against women and girls.* Vilnius, Lithuania: European Institute for Gender Equality.

European Union Agency for Fundamental Rights. 2013. *EU LGBT survey: European Union lesbian, gay, bisexual and transgender survey: Results at a glance.* Vienna, Austria: Publications Office of the European Union. https://fra.europa.eu/sites/default/files/eu-lgbt-survey-results-at-a-glance_en.pdf.

———. 2014. *Violence against women: an EU-wide survey: Main results.* Luxembourg City, Luxembourg: Publications Office of the European Union. https://fra.europa.eu/sites/default/files/fra_uploads/fra-2014-vaw-survey-main-results-apr14_en.pdf.

Evens, Emily, Michele Lanham, Karin Santi, Juana Cooke, Kathleen Ridgeway, Giuliana Morales, Caleb Parker, Claire Brennan, Marjan de Bruin, Pavel Chladni Desrosiers, Xenia Diaz, Marta Drago, Roger McLean, Modesto Mendizabal, Dirk Davis, Rebecca B. Hershow and Robyn Dayton. 2019. "Experiences of gender-based violence among female sex workers, men who have sex with men, and transgender women in Latin America and the Caribbean: a qualitative study to inform HIV programming." *BMC International Health and Human Rights* 19 (1): 1–14.

Fairbairn, Jordan. 2015. "Rape Threats and Revenge Porn: Defining Sexual Violence in the Digital Age." In *eGirls, eCitizens,* edited by Jane Bailey and Valerie Steeves, 229–52. Ottawa, ON: University of Ottawa Press.

Ferrier, Michelle. 2018. *Attacks and Harassment: The Impact on Female Journalists and Their Reporting.* TrollBusters and International Women's Media Foundation. www.iwmf.org/wp-content/uploads/2018/09/Attacks-and-Harassment.pdf.

Finlay, Alan, ed. 2013. *Global Information Society Watch 2013: Women's Rights, Gender and ICTs.* APC and Humanist Institute for Cooperation with Developing Countries. www.giswatch.org/sites/default/files/gisw13_chapters.pdf.

França, Leandro Ayres and Jessica Veleda Quevedo. 2020. "Project Leaked: Research on Non-Consensual Sharing of Intimate Images in Brazil." *International Journal of Cyber Criminology* 14 (1): 1–28.

Freed, Diana, Jackeline Palmer, Diana Elizabeth Minchala, Karen Levy, Thomas Ristenpart and Nicola Dell. 2017. "Digital Technologies and Intimate Partner Violence: A Qualitative Analysis with Multiple Stakeholders." *Proceedings of the ACM on Human-Computer Interaction* 1: 1–22.

Fry, Ellie. 2020. "Petition accusing PornHub of profiting from rape and abuse videos reaches 380,000 signatures." *The Independent,* March 20. www.independent.co.uk/life-style/pornhub-petition-rape-abuse-videos-petition-revenge-porn-a9388076.html.

Ging, Debbie. 2017. "Alphas, Betas, and Incels: Theorizing the Masculinities of the Manosphere." *Men and Masculinities* 22 (4): 638–57.

Goldberg, Carrie. 2019. *Nobody's Victim: Fighting Psychos, Stalkers, Pervs, and Trolls*. New York, NY: Plume.

Gurumurthy, Anita, Amrita Vasudevan and Nandini Chami. 2019. *Born digital, Born free? A socio-legal study on young women's experiences of online violence in South India*. Bangalore, India: IT for Change. https://itforchange.net/sites/default/files/1662/Born-Digital_Born-Free_SynthesisReport.pdf.

Hall, Matthew and Jeff Hearn. 2017. "Revenge pornography and manhood acts: a discourse analysis of perpetrators' accounts." *Journal of Gender Studies* 28 (2): 158–70.

Hellevik, Per and Carolina Øverlien. 2016. "Teenage intimate partner violence: Factors associated with victimization among Norwegian youths." *Scandinavian Journal of Public Health* 44 (7): 702–8.

Henry, Nicola and Asher Flynn. 2019. "Image-based sexual abuse: Online distribution channels and illicit communities of support." *Violence Against Women* 25 (16): 1932–55.

Henry, Nicola and Anastasia Powell. 2016. "Technology-Facilitated Sexual Violence: A Literature Review of Empirical Research." *Trauma, Violence, & Abuse* 19 (2): 195–208.

Henry, Nicola, Clare McGlynn, Asher Flynn, Kelly Johnson, Anastasia Powell and Adrian J. Scott. 2020. *Image-Based Sexual Abuse: A Study on the Causes and Consequences of Non-Consensual Nude or Sexual Imagery*. New York, NY: Routledge.

Human Rights Watch. 2020. "Egypt: Security Forces Abuse, Torture LGBT People." Human Rights Watch, October 1. www.hrw.org/news/2020/10/01/egypt-security-forces-abuse-torture-lgbt-people.

Inter-Parliamentary Union. 2016. "Sexism, harassment and violence against women parliamentarians." Issues brief, October. http://archive.ipu.org/pdf/publications/issuesbrief-e.pdf.

Iyer, Neema, Bonnita Nyamwire and Sandra Nabulega. 2020. *Alternate Realities, Alternate Internets: African Feminist Research for a Feminist Internet*. APC and International Development Research Centre. www.apc.org/sites/default/files/Report_FINAL.pdf.

James, Sandy E., Jody L. Herman, Susan Rankin, Mara Keisling, Lisa Mottet and Ma'ayan Anafi. 2015. *The Report of the 2015 U.S. Transgender Survey*. Washington, DC: National Center for Transgender Equality. www.transequality.org/sites/default/files/docs/USTS-Full-Report-FINAL.PDF.

Jane, Emma A. 2014. "'You're a Ugly, Whorish, Slut': Understanding E-bile." *Feminist Media Studies* 14 (4): 531–46.

———. 2018. "Gendered cyberhate as workplace harassment and economic vandalism." *Feminist Media Studies* 18 (4): 575–91.

Jeong, Sarah. 2018. *The Internet of Garbage*. Washington, DC: Vox Media. https://cdn.vox-cdn.com/uploads/chorus_asset/file/12599893/The_Internet_of_Garbage.0.pdf.

Khoo, Cynthia, Kate Robertson and Ronald Deibert. 2019. *Installing Fear: A Canadian Legal and Policy Analysis of Using, Developing, and Selling Smartphone Spyware and Stalkerware Applications*. Toronto, ON: Citizen Lab. https://citizenlab.ca/docs/stalkerware-legal.pdf.

Langlois, Ganaele and Andrea Slane. 2017. "Economies of reputation: the case of revenge porn." *Communications and Critical/Cultural Studies* 14 (2): 120–38.

Laub, Zachary. 2019. "Hate Speech on Social Media: Global Comparisons." Council on Foreign Relations, June 7. www.cfr.org/backgrounder/hate-speech-social-media-global-comparisons.

Laxton, Clare. 2014. *Virtual World, Real Fear: Women's Aid report into online abuse, harassment and stalking*. Bristol, UK: Women's Aid Federation of England. www.womensaid.org.uk/wp-content/uploads/2015/11/Women_s_Aid_Virtual_World_Real_Fear_Feb_2014-3.pdf.

Lenhart, Amanda, Michele Ybarra, Kathryn Zickuhr and Myeshia Price-Feeney. 2016. *Online Harassment, Digital Abuse, and Cyberstalking in America*. New York, NY: Data & Society Research Institute. www.datasociety.net/pubs/oh/Online_Harassment_2016.pdf.

Levy, Karen and Bruce Schneier. 2020. "Privacy Threats in Intimate Relationships." *Journal of Cybersecurity* 6 (1): 1–13.

Lewis, Ruth, Michael Rowe and Clare Wiper. 2016. "Online Abuse of Feminists as an Emerging Form of Violence Against Women and Girls." *British Journal of Criminology* 57 (6): 1462–81.

Mafa, Itai, Simon Kang'ethe and Victor Chikadzi. 2020. "'Revenge Porn' and Women Empowerment Issues: Implications for Human Rights and Social Work Practice in Zimbabwe." *Journal of Human Rights and Social Work* 5 (2): 118–28.

Malanga, Donald Flywell. 2020. "Tackling Gender-based Cyber Violence against Women and Girls in Malawi amidst the COVID-19 Pandemic." African Declaration on Internet Rights and Freedoms, June 28. https://africaninternetrights.org/en/updates/tackling-gender-based-cyber-violence-against-women-and-girls-malawi-amidst-covid-19-pandemic.

Maple, Carsten, Emma Short and Antony Brown. 2011. *Cyberstalking in the United Kingdom: An Analysis of the ECHO Pilot Survey*. Bedfordshire, UK: University of Bedfordshire.

Martin, Noelle. 2017. "Online predators spread fake porn of me. Here's how I fought back." TEDxPerth, November. www.ted.com/talks/noelle_martin_online_predators_spread_fake_porn_of_me_here_s_how_i_fought_back?language=en.

Marwick, Alice E. 2017. "Scandal or sex crime? Gendered privacy and the celebrity nude photo leaks." *Ethics and Information Technology* 19 (1): 177–91.

Marwick, Alice E. and Robyn Caplan. 2018. "Drinking male tears: language, the manosphere, and networked harassment." *Feminist Media Studies* 18 (4): 543–59.

Masoodi, Ashwaq. 2016. "The business of rape videos." *Mint,* August 9. www.livemint.com/Politics/QbMrC4xptoWj84iGE86ETI/The-business-of-rape-videos.html.

Massanari, Adrienne. 2017. "#Gamergate and the Fappening: How Reddit's algorithm, governance, and culture support toxic technocultures." *New Media & Society* 19 (3): 329–46.

McGlynn, Clare and Erika Rackley. 2017. "Image-Based Sexual Abuse." *Oxford Journal of Legal Studies* 37 (3): 534–61.

McGlynn, Clare, Erika Rackley and Ruth Houghton. 2017. "Beyond 'revenge porn': The continuum of image-based sexual abuse." *Feminist Legal Studies* 25 (1): 25–46.

McPhate, Mike. 2016. "Teenager Is Accused of Live-Streaming a Friend's Rape on Periscope." *The New York Times,* April 18. www.nytimes.com/2016/04/19/us/periscope-rape-case-columbus-ohio-video-livestreaming.html.

Milligan, Shelly. 2011. "Criminal harassment in Canada, 2009." Statistics Canada, March 3. www150.statcan.gc.ca/n1/pub/85-005-x/2011001/article/11407-eng.pdf.

Mishra, Smeeta and Surhita Basu. 2014. "Family honor, cultural norms and social networking: Strategic choices in the visual self-presentation of young Indian Muslim women." *Cyberpsychology: Journal of Psychosocial Research on Cyberspace* 8 (2): Article 3.

Nakamura, Lisa. 2013. "'It's a nigger in here! Kill the nigger!' User-generated media campaigns against racism, sexism, and homophobia in digital games." In *The International Encyclopedia of Media Studies,* vol. VI: *Media Studies Futures,* edited by Kelly Gates, 1–15. Malden, MA: Wiley-Blackwell.

National Network to End Domestic Violence. 2014. "A Glimpse From the Field: How Abusers Are Misusing Technology." Washington, DC: National Network to End Domestic Violence.

Netsafe. 2020. "Understanding fake sextortion email scams." Netsafe, April 2. www.netsafe.org.nz/faketortian-email-scam/.

Office of the Chief Coroner. 2011. *Domestic Violence Death Review Committee — 2010 Annual Report.* Toronto, ON: Province of Ontario.

Organization for Security and Co-operation in Europe. 2016. *Countering Online Abuse of Female Journalists.* Vienna: Organization for Security and Co-operation in Europe. www.osce.org/files/f/documents/c/3/220411.pdf.

Paling, Emma. 2015. "Wikipedia's Hostility to Women." *The Atlantic,* October 21. www.theatlantic.com/technology/archive/2015/10/how-wikipedia-is-hostile-to-women/411619/.

Palmer, Tanya. 2018. "Rape pornography, cultural harm and criminalization." *Northern Ireland Legal Quarterly* 69 (1): 37–58.

Parsons, Christopher, Adam Molnar, Jakub Dalek, Jeffrey Knockel, Miles Kenyon, Bennett Haselton, Cynthia Khoo and Ronald Deibert. 2019. *The Predator in Your Pocket: A Multidisciplinary Assessment of the Stakerware Application Industry.* Citizen Lab. https://citizenlab.ca/docs/stalkerware-holistic.pdf.

Pasricha, Japleen. 2016. "'Violence' Online in India: Cybercrimes Against Women & Minorities on Social Media." Feminism in India, May 18. https://feminisminindia. com/wp-content/uploads/2016/05/FII_cyberbullying_report_website.pdf.

Plan International. 2020. *Free to be online? Girls' and young women's experiences of online harassment.* Surrey, UK: Plan International. https://plan-international.org/publications/freetobeonline.

Posetti, Julie. 2020. "New study will explore online violence against women journalists." International Journalists' Network, September 25. https://ijnet.org/en/story/new-study-will-explore-online-violence-against-women-journalists.

Powell, Anastasia and Nicola Henry. 2017. *Sexual Violence in a Digital Age.* London, UK: Palgrave MacMillan.

Powell, Anastasia, Nicola Henry, Asher Flynn and Adrian J. Scott. 2018. "Image-based sexual abuse: The extent, nature, and predictors of perpetration in a community sample of Australian adults." *Computers in Human Behavior* 92: 393–402.

Reporters Without Borders. 2018. *Online Harassment of Journalists: Attack of the Trolls.* Paris: Reporters Without Borders. https://rsf.org/sites/default/files/rsf_report_on_online_harassment.pdf.

Ruiz-Navarro, Catalina. 2016. "Political Violence is Directly Linked to Online Harassment." Women's Media Centre, April 22. www.womensmediacenter.com/speech-project/political-violence-directly-linked-online-harassment-catalina-ruiz-navarro.

Safety Net Canada. 2013. *Assessing Technology in the Context of Violence Against Women & Children: Examining Benefits & Risks.* Vancouver, BC: Safety Net Canada. https://bcsth.ca/wp-content/uploads/2016/10/Assessing-Technology-in-the-Context-of-Violence-Against-Women-Children.-Examining-Benefits-Risks..pdf.

Salter, Michael. 2017. "From geek masculinity to Gamergate: the technological rationality of online abuse." *Crime, Media, Culture. An International Journal* 14 (2): 247–64.

Salter, Michael and Thomas Crofts. 2015. "Responding to Revenge Porn: Challenges to Online Legal Impunity." In *New Views on Pornography: Sexuality, Politics, and the Law,* edited by Lynn Comella and Shira Tarrant, 233–53. Santa Barbara, CA: Praeger.

Sambasivan, Nithya, Amna Batool, Nova Ahmed, Tara Matthews, Kurt Thomas, Laura Sanely Gaytán-Lugo, David Nemer, Elie Bursztein, Elizabeth Churchill and Sunny Consolvo. 2019. "'They Don't Leave Us Alone Anywhere We Go': Gender and Digital Abuse in South Asia." CHI '19: Proceedings of the 2019 CHI Conference on Human Factors in Computing Systems, May 4–9.

Slane, Andrea and Ganaele Langlois. 2018. "Debunking the Myth of 'Not My Bad': Sexual Images, Consent, and Online Host Responsibilities in Canada." *Canadian Journal of Women and the Law* 30 (1): 42–81.

Solove, Daniel J. 2007. *The Future of Reputation: Gossip, Rumor, and Privacy on the Internet.* New Haven, CT: Yale University Press.

Srivastava, Roli. 2017. "From streets to smartphones: India grapples with online rape." Reuters, November 15. https://fr.reuters.com/article/us-india-women-rape-idUSKBN1DF0UN.

Statistics Canada. 2017. "Cyberstalking in Canada." Statistics Canada, December 4. www150.statcan.gc.ca/n1/pub/11-627-m/11-627-m2017039-eng.htm.

Staude-Müller, Frithjof, Britta Hansen and Melanie Voss. 2012. "How stressful is online victimization? Effects of victim's personality and properties of the incident." *European Journal of Developmental Psychology* 9 (2): 260–74.

Sundén, Jenny and Susanna Paasonen. 2018. "Shameless hags and tolerance whores: feminist resistance and the affective circuits of online hate." *Feminist Media Studies* 18 (4): 643–56.

The eQuality Project. 2020. "Tech-Facilitated Violence — Criminal Case Law." www.equalityproject.ca/resources/tfv-criminal-case-law/.

The Guardian. 2016. "The dark side of Guardian comments." *The Guardian,* April 12. www.theguardian.com/technology/2016/apr/12/the-dark-side-of-guardian-comments.

Thomasen, Kristen. 2018. "Beyond airspace safety: A feminist perspective on drone privacy regulation." *Canadian Journal of Law and Technology* 16 (2): 307–38.

Thomasen, Kristen and Suzie Dunn. Forthcoming 2021. "Reasonable Expectations of Privacy in an Era of Drones and Deepfakes: Expanding the Supreme Court of Canada's Decision in *R v Jarvis.*" In *The Emerald International Handbook of Technology-Facilitated Violence and Abuse,* edited by Asher Flynn, Nicola Henry and Jane Bailey. Bingley, UK: Emerald Publishing Ltd.

Thompson, Chrissy and Mark A. Wood. 2018. "A media archaeology of the creepshot." *Feminist Media Studies* 18 (4): 560–74.

Thorsen, Einar and Chindu Sreedharan. 2019. "#EndMaleGuardianship: Women's rights, social media and the Arab public sphere." *New Media & Society* 21 (5): 1121–40.

Udwadia, Zarah and Baldeep Grewal. 2019. *Free To Be Mobile.* Mumbai, India: Point of View. www.apc.org/sites/default/files/FTBM_Web_final.pdf.

Uhl, Carolyn A., Katlin J. Rhyner, Cheryl A. Terrance and Noël R. Lugo. 2018. "An examination of nonconsensual pornography websites." *Feminism & Psychology* 28 (1): 50–68. doi:10.1177/0959353517720225.

UN. 1993. *Declaration on the Elimination of Violence against Women.* 48th sess. A/RES/48/104. December 20.

———. 2017. Committee on the Elimination of Discrimination against Women. *General Recommendation No. 35 on gender-based violence against women, updating General Recommendation No. 19.* CEDAW/C/GC/35. July 14.

———. 2018. *Report of the Special Rapporteur on violence against women, its causes and consequences on online violence against women and girls from a human rights perspective.* 38th sess. A/HRC/38/47. June 16.

UN OHCHR. 2017. "UN experts urge States and companies to address online gender-based abuse but warn against censorship." OHCHR news release, March 8. www.ohchr.org/EN/NewsEvents/Pages/DisplayNews.aspx?NewsID=21317.

———. 2018. "UN experts call on India to protect journalist Rana Ayyub from online hate campaign." OHCHR news release, May 24. www.ohchr.org/EN/NewsEvents/Pages/DisplayNews.aspx?NewsID=23126&LangID=E.

UN Women. 2020a. "COVID-19 and Ending Violence Against Women and Girls: Addressing the Shadow Pandemic." Policy Brief No. 17.

———. 2020b. "Online and ICT-facilitated violence against women and girls during COVID-19." Brief.

Valente, Mariana Giorgetti, Natália Neris and Lucas Bulgarelli. 2015. "Not Revenge, Not Porn: Analysing the Exposure of Teenage Girls Online in Brazil." Global Information Society Watch.

Valente, Mariana Giorgetti, Natália Neris, Juliana Pacetta Ruiz and Lucas Bulgarelli. 2018. *The Body is Code: Legal Strategies to Combat Revenge Porn in Brazil.* São Paolo: Internet Lab.

Valle, Firuzeh Shokooh. 2020. "Turning fear into pleasure: feminist resistance against online violence in the Global South." *Feminist Media Studies.*

Van der Wilk, Adriane. 2018. *Cyber violence and hate speech online against women.* PE 604.979. Brussels, Belgium: European Parliament. www.europarl.europa.eu/RegData/etudes/STUD/2018/604979/IPOL_STU(2018)604979_EN.pdf.

Vanity Fair. 2014. "Cover Exclusive: Jennifer Lawrence Calls Photo Hacking a 'Sex Crime.'" *Vanity Fair,* October 7. www.vanityfair.com/hollywood/2014/10/jennifer-lawrence-cover.

Veletsianos, George, Shandell Houlden, Jaigris Hodson and Chandell Gosse. 2018. "Women scholars' experiences with online harassment and abuse: Self-protection, resistance, acceptance, and self-blame." *New Media & Society* 20 (12): 4689–708.

Vera-Gray, Fiona and Liz Kelly. 2020. "Contested gendered space: public sexual harassment and women's safety work." *International Journal of Comparative and Applied Criminal Justice* 44 (4): 265–75.

Waldman, Ari Ezra. 2017. "A Breach of Trust: Fighting 'Revenge Porn.'" *Iowa Law Review* 102: 709–33.

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

Wikimedia. 2018. "Community Insights/2018 Report/Contributors." https://meta.wikimedia.org/wiki/Community_Insights/2018_Report/Contributors.

Wirtz, Andrea L., Tonia C. Poteat, Mannat Malik and Nancy Glass. 2018. "Gender-Based Violence Against Transgender People in the United States: A Call for Research and Programming." *Trauma, Violence, & Abuse* 21 (2): 227–41.

Witness Media Lab. 2016. *Capturing Hate: Eyewitness Videos Provide New Source of Data on Prevalence of Transphobic Violence.* Witness Media Lab, October. www.issuelab.org/resources/25865/25865.pdf.

Wittes, Benjamin, Cody Poplin, Quinta Jurecic and Clara Spera. 2016. *Sextortion: Cybersecurity, teenagers, and remote sexual assault.* Brookings Institute, May. www.brookings.edu/research/sextortion-cybersecurity-teenagers-and-remote-sexual-assault/.

Wolak, Janis and David Finkelhor. *Sextortion: Findings from a Survey of 1,631 Victims.* Durham, NH: University of New Hampshire. www.unh.edu/ccrc/pdf/Sextortion_RPT_FNL_rev0803.pdf.

Women's Legal and Human Rights Bureau, Inc. 2015. "From impunity to justice: Domestic legal remedies for cases of technology-related violence against women." Women's Legal and Human Rights Bureau, Inc., March 3. www.genderit.org/sites/default/files/impunity_womens_legal_dig_0.pdf.

Wood, Elisabeth Jean. 2018. "Rape as a Practice of War: Toward a Typology of Political Violence." *Politics & Society* 46 (4): 513–37.

Woodlock, Delanie. 2015. *ReCharge: Women's Technology Safety, Legal Resources, Research and Training.* Women's Legal Service NSW, Domestic Violence Resource Centre Victoria and WESNET. www.dvrcv.org.au/sites/default/files/ReCharge_0.pdf.

World Health Organization. 2013. *Global and regional estimates of violence against women: prevalence and health effects of intimate partner violence and non-partner sexual violence.* Geneva, Switzerland: World Health Organization Press.

World Wide Web Foundation. 2014. "The Web in 2014: Less Free, More Unequal, Warns World Wide Web Foundation in Annual Web Index." World Wide Web Foundation press release, December 11. http://thewebindex.org/wp-content/uploads/2014/12/WebIndex2014GlobalPressRelease.pdf.

Younes, Rasha. 2020. "This Pride Month, Shame on You: Exposing Anti-LGBT Government Strategies in MENA." Human Rights Watch, June 8. www.hrw.org/news/2020/06/08/pride-month-shame-you-exposing-anti-lgbt-government-strategies-mena.

YWCA. 2017. "Technology and Gender-Based Violence." YWCA, September. www.ywca.org/wp-content/uploads/WWV-Technology-and-GBV-Fact-Sheet.pdf.

Centre for International
Governance Innovation

67 Erb Street West
Waterloo, ON, Canada N2L 6C2
www.cigionline.org

@cigionline