Technology-facilitated Gender-based Violence

Making all spaces safe

Technical Division
December 2021

Technology-facilitated Gender-based Violence

Making all spaces safe

December 2021

Acknowledgements

As the world continues to evolve and expand in the use of technology and platforms, so too does the expansion of spaces through which violence can be perpetrated. This was evidenced no more so than during the COVID-19 pandemic where containment efforts reduced access to information and services driving increased use of technology and online spaces. This paper serves as an alarm bell for the international community, digital and feminist movements, private technology companies and national Governments to act in unison to end the rising scourge of technology-facilitated gender-based violence.

On behalf of the UNFPA, the United Nations Population Fund wish to acknowledge the contribution of their valuable time and expertise in discussions and technical review including Dr Suzie Dunn, Assistant Professor in Law & Technology at Dalhousie University's Schulich School of Law, Sophie Read-Hamilton, Independent GBV Consultant and Chandra Pauline Daniel Ph.D. Doctorate Program in Public Health-Health Policy & Management, New York Medical College; Strategic Plan Results Analysis Intern- PSIPB-Policy and Strategy Division, UNFPA.

This report was produced by the UNFPA Technical Division, Gender and Human Rights Branch under the technical leadership of Alexandra Robinson. Co-authors of the paper are Alexandra Robinson and Nora Piay- Fernandez with review from Sarah Baird, Mar Jubero, Dawn Minott and Jude Larnerd.

Table of contents:

Part 1

What is TFGBV?

Definition, Prevalence and Impact

Background

The emergence of, and the increasing reliance on digital technology and spaces, is a global megatrend,[1] a universal phenomenon that is shaping our current world. Digitalization is driving structural changes in how people communicate, work, learn, produce and consume. Technological innovation and digitalization are opening a window of opportunities for sustainable development, in a time when many aspects of human life are being radically transformed.[2] Technology has the potential to foster economic growth; to expand access to education, information and knowledge; and to give voice and power to those furthest left behind and those whose voices were not traditionally heard, thereby enhancing participation in public life and democratic processes.

However, while the digitalization of the world represents significant opportunity, it is also a space through which harm may be perpetrated. Research indicates that at least 38 per cent of women globally have personally experienced online violence and that this rate is rising.[3] Technology-facilitated gender-based violence (TFGBV) targets all women who use technology, including both cis and trans women and people who present as feminine, non-binary or gender-diverse individuals.[4] Certain groups of women are at a higher risk because of what they do, who they are or if they access certain information and services. This includes women journalists, politicians, women activists and feminists, academics and young people for example.[5] Of those adolescent girls who do have access to digital technologies, 64 per cent are high users and are particularly vulnerable to TFGBV.[6] The violence against women and girls is more frequent if they have a disability, are racialized, LGBTQIA+, socioeconomically disadvantaged and/or politically outspoken.[7]

In the words of the Women's Legal Education and Action Fund:

> [t]he ubiquity of the Internet means that TFGBV can become omnipresent and relentless, infiltrating a victim's most intimate physical spaces, such as their home or bedroom. Users engaging in TFGBV can also leverage their own and targeted individuals' online social networks to further the abuse, by recruiting others to knowingly or unwittingly share abusive material, and by contaminating the targeted individuals' own online spaces and communities. The online permanence of abusive material – which is exceedingly difficult to completely eradicate once shared online – also ensures continued revictimization, resulting in lasting psychological and other damage.[8]

Furthermore, TFGBV can take many forms and is committed across a continuum. That is, it is committed as part of a pattern of violence perpetrated both online and offline.[9]

Addressing TFGBV, as a growing area of critical concern, is no longer negotiable. Ensuring that everyone can freely participate online and without fear of violence and abuse is vital to ensuring that women can effectively exercise their right to freedom of expression. The United Nations Human Rights Council stated that "the same rights people have offline must also be protected online, in particular freedom of expression, which is applicable regardless of frontiers and through any media of one's choice, in accordance with articles 19 of the Universal Declaration of Human Rights and the International Covenant on Civil and Political Rights".[10]

More specifically, the principle that human rights and women's rights protected offline must also be protected online should fully integrate the right to live free from emerging forms of online and information and communication technologies-facilitated violence against women, while respecting the right to freedom of expression and the right to privacy and data protection.[11]

The use of technology and online spaces should serve as a tool for accelerating the achievement of gender equality and the empowerment of women instead of a tool of subjugation, the perpetration of violence and silencing of women in all their diversity.

Defining TFGBV

There is a lack of consensus globally on a definition of violence that is perpetrated using technology and committed through online and digital spaces.[12] A well-established, internationally-accepted and standardized definition of TFGBV is critical to provide a common understanding to enable standardized measurement and minimum standards for response and prevention.

In order to contribute to this critical gap in knowledge, UNFPA has reviewed terms and definitions published by international organizations, scholars and civil society organizations in the past five years and has proposed a new working definition. Building on these definitions and their complementarity, UNFPA proposes to adapt the term technology-facilitated abuse to the broader term of TFGBV, defined as follows:

> An act of violence perpetrated by one or more individuals that is committed, assisted, aggravated and amplified in part or fully by the use of information and communication technologies or digital media,[13] against a person on the basis of their gender.

This comprehensive working definition has been chosen because (1) it highlights the gendered nature of the violence and (2) it is inclusive of the circumstances and forms in which technology can be used to perpetrate violence. This broad and inclusive definition encompasses existing patterns of violence, harassment and abuse, as well as new forms of abuse, such as image-based abuse (IBA). Furthermore, this terminology allows to differentiate "*online violence*" or "*digital violence*", as the violence that is perpetrated against women in online spaces or through digital media, from "*technology-facilitated violence*", which is perpetrated by any type of technological means, information and communications technology and digital media, including phones, Global Positioning System (GPS) tracking devices, drones and non-Internet connected recording devices.

Characteristics of TFGBV

TFGBV shares common characteristics with other forms of gender-based violence:

- It occurs in all societies worldwide
- It is gendered and rooted in gender inequality thereby disproportionately impacting women and girls in all their diversity
- It can have severe impacts on the health, well-being and lives of survivors

digital nature

TFGBV also has distinct characteristics related to its digital nature:[14]

Anonymity
The perpetrator or abuser can remain anonymous.

Action at a distance
It can be perpetrated at a distance, from anywhere in the world and without personal or physical contact with the survivor.

Accessibility and affordability
It is accessible and affordable to perpetrators, since information and communications technology have reduced the cost and difficulty of producing and distributing information at scale.

Propagation
It is constant and easily propagated through the Internet, retraumatizing survivors. The ease, efficiency and affordability of automating and multiplying instances of abuse against a particular group or individual means that it is an effective form of violence in wielding harm.

Impunity
It is often perpetrated with impunity. Given that TFGBV can be committed anonymously and from a distance, there are difficulties in law enforcement across countries and jurisdictions that limit judicial systems' ability to hold abusers accountable for their actions.

Automation
It can be automatic and easy to perpetrate, and allows perpetrators to control women's movements, monitor their online activity and distribute images or information, among other harmful abusive actions, with limited time and effort.

Collectivity
It can be collectively organized and perpetrated by a large number of individuals.

Normalization of violence
TFGBV contributes to the normalization of violence against women and girls. Physical violence against women is often normalized and justified, particularly by women themselves. In fact, across 49 low- and middle-income countries, 41 per cent of women and 32 per cent of men justify domestic physical violence in at least one circumstance.[15] It is likely that this normalization of violence is exacerbated in the digital space, and that TFGBV is perceived as less serious, harmful or dangerous to survivors.

Perpetuity
It can be committed in perpetuity, as images and digital materials used to perpetrate abuse are likely to exist indefinitely or for long periods of time.

Forms of TFGBV

TFGBV is "carried out through text, images and unwanted digitally-enabled or enhanced surveillance and monitoring, using a variety of devices and platforms from basic digital tools, such as texting, email and social media, to more advanced technologies such as artificial intelligence (AI), GPS tracking and drones".[16] As new technologies and digital spaces become available, new forms of TFGBV emerge, such as the use of AI for IBA or stalking using GPS tracking on cellular phone devices.[17] At the same time, old technologies are used to perpetrate violence in new ways. For example, in the context of abusive intimate relationships, perpetrators are using Internet bank transfers to send harassing messages to survivors.[18]

Some of the most common forms of TFGBV include, but are not limited to, the following:[19]

1 Online harassment, including online gender and sexual harassment

Online harassment is the use of technology to repeatedly contact, annoy, threaten or scare another person. Online harassment is an ongoing behaviour over time rather than an isolated incident.[20] Online harassment can be perpetrated by a single individual or mobs of individuals (*mobbing*), usually networks of male perpetrators who target women and minorities.[21] When online harassment is perpetrated on the basis of the survivor's gender, sexuality or sexual orientation it constitutes a form of TFGBV.[22]

Online sexual harassment is a specific form of harassment that may involve unwanted sexual attention and sexual coercion.[23] It has also been defined as "any unwanted sexual behaviour via electronic means and can include unwanted sexual solicitation; unwanted requests to talk about sex; unwanted requests to do something sexual online or in person; receiving unwanted sexual messages and images; having sexual messages and images shared without permission; and revealing identifying and personal information about a person online".[24]

Cyberstalking, tracking or cyberobsessive pursuit and surveillance

2

Cyberstalking is "the use of technology to stalk and monitor someone's activities and behaviours in real-time or historically".[25] Cyberstalking is usually seen as an extension of offline stalking, using technological tools, and it involves a set of unwanted, repetitive, intrusive, threatening and harassing behaviours, which in some instances are seen as a relatively normal relational or dating practice. Some scholars use the term "cyberobsessional pursuit" to refer to the "unwanted pursuit of intimacy through a repeated invasion of a person's sense of physical or symbolic intimacy, using digital or online means", and consider cyberstalking a severe form of cyberobsessional pursuit and surveillance, which may be motivated by relational control or destruction and cause the survivor to feel fear.[26]

Cyberstalking involves, for example, monitoring or tracking a person's location and/or activities using GPS trackers, spyware,[27] cameras and microphones, and location-based dating apps, checking email, call or message histories, as well as monitoring a person's social media profiles.[28]

IBA

3

IBA consists of "using images to coerce, threaten, harass, objectify or abuse". One form of IBA is image-based sexual abuse (IBSA),[29] which involves at least one of three behaviours: taking, sharing or threatening to share sexually explicit images without consent. Some scholars have argued for the inclusion of other forms of gendered and sexualized abuse, perpetrated using technological tools, such as *upskirting*, or non-consensually taking an image up a person's skirt or dress; *deepfakes*, or non-consensually created sexual imagery that depict the victim in a sexual way, usually developed using AI tools; and *cyberflashing*, or sending unsolicited images of their own genitals to another person.[30] Other examples include photographing or filming someone without their consent or knowledge,[31] or coercing someone to engage in unwanted sexual behaviour online.[32]

Technology-facilitated sexual abuse

Technology-facilitated sexual abuse refers to the use of communication technologies, such as cell phones, email, social networking sites, chat rooms or online dating sites and apps, to commit or procure sexual assault or abuse.[33] Generally, technology-facilitated unwanted sexual experiences involve three distinct behaviours: (1) sextortion, or coercing someone into a sexual activity through blackmail, bribery or threats to release intimate images or sensitive information; (2) using technology to contact a potential victim, such as through dating apps, to then perpetrate a sexual offence; and (3) "rape by proxy", when offenders solicit and arrange a third party to sexually assault a person, often using a false identity or pretending to be the victim.[34] Additionally, technology-facilitated sexual abuse may involve "sexting coercion", by which the offenders force someone into engaging in unwanted sexually explicit texting, or sharing of images and videos; and "unwanted sexual solicitation", receiving unwanted requests to talk about sex or do something sexual.[35]

Online grooming is another specific type of technology-facilitated sexual abuse where children and young people are contacted through social media or other digital platforms, with the purpose of sexually assaulting them. It has been defined as a "process by which a perpetrator prepares a child, significant adults and the environment for the abuse. This includes gaining access to the child, gaining the child's compliance and maintaining the child's secrecy to avoid disclosure".[36]

Doxxing or doxing

Doxxing is the non-consensual disclosure of personal information. It involves the public release of an individual's private, personal, sensitive information, such as home and email addresses, phone numbers, employer and family member's contact information, or photos of their children and the school they attend.[37] Doxxing is a form of online harassment that rarely occurs in isolation, rather it is accompanied with other forms of harassment such as IBA.[38] Women, especially from minority groups, are more likely to be subjected to doxxing, which disproportionately impacts women of colour and LGTBQI+ communities.[39]

According to Douglas, there are three types of doxxing: de-anonymizing, or revealing someone's identity; targeting, or revealing someone's personal and private information that allows her to be physically located, the consequences of which are gendered and may pose serious security implications for most women; and de-legitimizing, releasing private information in order to undermine someone's credibility or reputation and to shame and humiliate them.[40] Doxxing often leads to further online and physical harassment, such as receiving large amounts of abusive messages and threats by email, phone or post.[41]

Hacking

Hacking is defined as the "use of technology to gain illegal or unauthorized access to systems or resources for the purpose of acquiring personal information, altering or modifying information, or slandering and denigrating the survivor and/or violence against women's organizations".[42] The survivor's personal computer or cellular phone may be hacked to obtain intimate images to perpetrate IBA, blackmail or coerce them into an unwanted sexual activity; or to obtain private information that may be used for doxxing or other violent acts.[43] Perpetrators can also hack a survivor's email and social media accounts to control their online activity, or even access bank accounts and control the survivor's finances and/or financially harm them.[44] Hackers may also target women's rights organizations, activists or public figures' online spaces because of their views on feminism, gender equality or sexual rights, thereby limiting women's participation in online forums and hindering their rights.[45]

Recruitment and the use of technology to locate survivors in order to perpetrate violence

Technology may be used to lure potential victims/survivors into violent situations[46] or to facilitate in-person physical or sexual assault.[47] Perpetrators and traffickers may use technology to contact potential victims through fraudulent posts and advertisements in dating sites and apps, "marriage agencies" or publish false employment and study opportunities.[48] Certain technology, such as spyware or GPS tracking, may also be used by perpetrators of IPV to track the movement and activities of survivors, monitor, control and locate them, with the purpose of intimidating or physically assaulting them.[49]

This form of violence is also evident in the way in which women, young people and children are lured into trafficking.[50] There have also been known cases of young people, children and adolescents, particularly girls, who have been recruited online by Islamic State of Iraq and Syria (ISIS) through social media, and lured into marriage under the promise of a utopian life.[51]

Impersonation

Impersonation is the process of stealing someone's identity so as to threaten or intimidate, as well as to discredit or damage a user's reputation.[52] Perpetrators may take over or create fake online accounts and websites of women to spread false information and damage their reputation,[53] to ruin their personal and/or professional relationships,[54] to call for violence against them through sex work advertisements or dating apps[55] or to obtain information about the survivor.[56] Impersonation may be perpetrated by individual abusers, but also by State actors. For example, State actors have the capacity to create false accounts on social media or impersonate others with the purpose of prosecuting minorities and certain groups, such as LGBTQIA+ people.[57]

Hate speech

Hate speech is “any kind of communication in speech, writing or behaviour, that attacks or uses pejorative or discriminatory language with reference to a person or a group on the basis of who they are, in other words, based on their religion, ethnicity, nationality, race, colour, descent, gender or other identity factor”.[58] Online hate speech based on gender and/or sexual orientation reinforces systemic sexism while dehumanizing and encouraging violence against women and girls. In recent years, hate speech against women, girls and LGTBQI+ people has increased considerably, with social media platforms and online chat forums hosting groups who promote hatred and violence against women.[59]

10

Defamation

Defamation involves the public release of false information that damages a person's reputation and that has the intention of humiliating, threatening, intimidating or punishing the survivor.[60] Given the strict gender norms that govern female sexuality, defamatory statements about women's sexuality are particularly harmful to survivors' reputations. In fact, most online defamatory attacks against women and girls often focus on their sexuality.[61]

11

Limiting or controlling use of technology

In abusive intimate relationships particularly, perpetrators may use technology to exert abuse and control over the survivor, by tracking, monitoring or restricting survivor's movements, communications and activities. These abusive behaviours include forcing their partners to give their passwords, obtaining unauthorized access to their online accounts, limiting their use of technology devices by digitally or physically controlling access to devices or accounts and inspecting survivor's devices. Intimate partners and family members have greater access to a person's devices, personal information and can exert coercive power and control over them. For example, intimate partners may know and monitor each other's bank accounts, social media and share passwords and devices, willingly or unwillingly, with one another. In abusive intimate relationships, intimate privacy threats to technology use can be a precursor to other forms of abuse.[62]

Prevalence of TFGBV

Increasingly research is becoming available that highlights the prevalence of forms of TFGBV. However, this research uses different methodologies and survey tools as well as targets different population groups and measures specific forms of TFGBV.

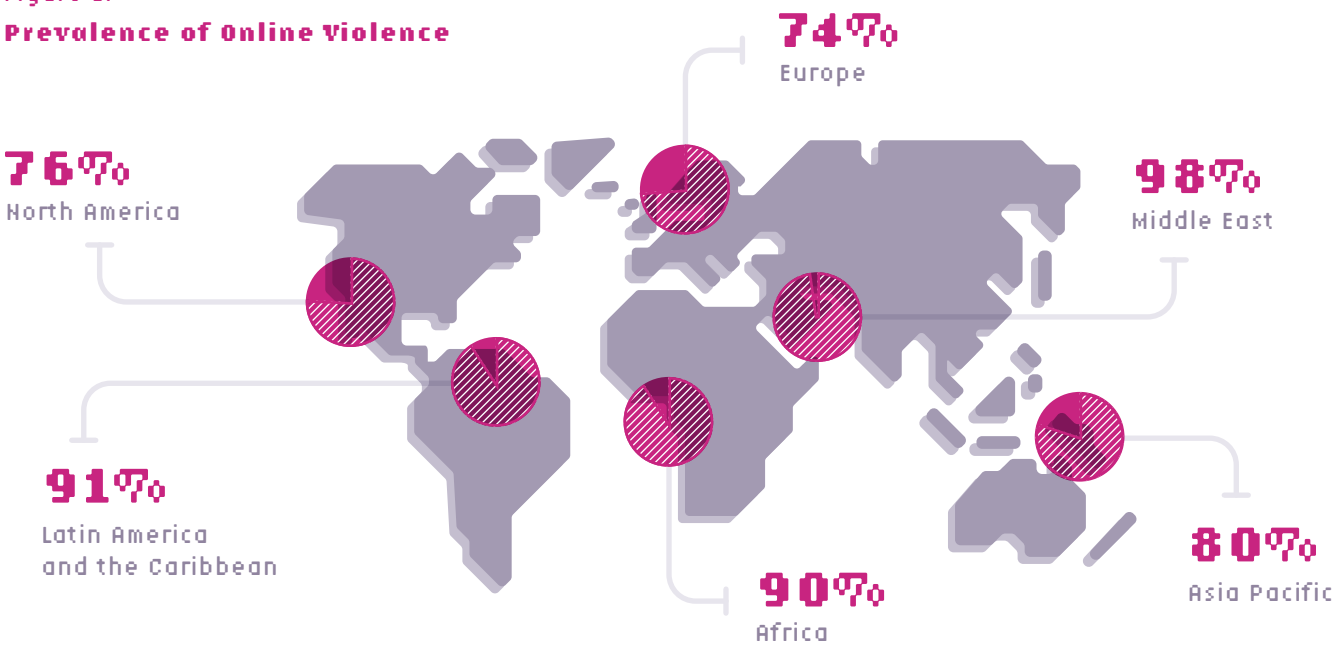
Measuring the extent and the impact of violent acts committed online and/or through digital and technological means is a daunting task, for a number of reasons:

- The absence of a standardized definition of TFGBV and its various forms;
- Prevalence may be measured in a way that fails to take account of the level of accessibility to technology and digital spaces for women and girls;
- The ever-emerging forms of TFGBV as new technologies emerge, old technologies are used differently and new digital and online spaces become available.

Combined, this means that there is no single validated quantitative measure relied upon to obtain prevalence data at local, national, regional and global levels[63] to support evidence-based policy, programme interventions (response and prevention) as well as accountability measures.

A recent study conducted by the Economist Intelligence Unit in 2021 among women in the 51 countries with the highest Internet penetration rates[64] has shown that, globally, 38 per cent of women with Internet access have personally experienced online violence, 63 per cent of women know someone who had been subjected to it and 85 per cent of women have witnessed online violence being perpetrated against another woman.[65] This study also offered regional estimates for the prevalence of online violence against women, as represented in Figure 1.

Figure 1.
Prevalence of Online Violence



Our study covered the top 51 countries by number of persons online
Source: https://onlineviolencewomen.eiu.com/

It is likely that these results underestimate the actual prevalence of TFGBV, given that this study only considered online violence and did not include other forms of technology-facilitated violence perpetrated via mobile phones, GPS and other technologies. It also only included women and not adolescents who are likely at higher risk of TFGBV. Indeed, a study conducted by Plan International among young women and adolescent girls (aged 15–25 years) from 31 countries worldwide highlighted the higher and more frequent use of social media by younger generations, thereby increasing exposure to TFGBV. The report found that 58 per cent of women and girls aged 15–25 years had experienced online harassment.[66]

Although not comprehensive, an extensive review of surveys has been conducted and contained in Part 3. Although the body of research is small, studies generally do not measure the TFGBV in its most inclusive form, but examine and measure specific forms of TFGBV. Further, the data are limited to localized studies with relatively small sample sizes.

The pervasive nature of TFGBV is a significant cause for concern. The data indicate prevalence estimates of online abuse as high as 58 per cent,[67] which is far in excess of current global estimates of the lifetime experience of IPV and non-partner sexual violence which is 31 per cent of women aged 15–49 years.[68]

This suggests that where Internet penetration rates are high and women and girls access technology, rates of TFGBV are almost double the rates of IPV. As Internet penetration and access to technologies increase, these trends are set to increase.

In addition to prevalence of TFGBV, some data have been collected around attitudes towards the impact of online harassment. Findings from the United States have shown a gendered difference in attitudes where half of women confirm that offensive content online is too often excused as not significant whereas 64 per cent of men, and 73 per cent of young men, state that offensive content online is taken too seriously.[69] Although limited in scope, this research, like the prevalence data available, creates cause for concern requiring similar survey work around attitudes be undertaken on a broader scale.

Available prevalence data combined with limited understanding of the impacts of TFGBV and the lack of accountability mechanisms and coordinated responses paints a bleak picture of the current state of perpetration and response to TFGBV. It is critical that standardized definitions and data-collection methodologies related to TFGBV are agreed upon to provide a robust evidence base moving forward.

58% 31%

The data indicate prevalence estimates of online abuse as high as 58 per cent, which is far in excess of current global estimates of the lifetime experience of IPV and non-partner sexual violence which is 31 per cent of women aged 15–49 years.

Who experiences TFGBV?

Although women and girls are most at risk of TFGBV, specific groups of women and girls are disproportionately targeted. This includes women with disabilities, adolescent girls, women of colour, women in public life such as women journalists or politicians and LGBTQIA+ persons.[70]

Adolescent girls

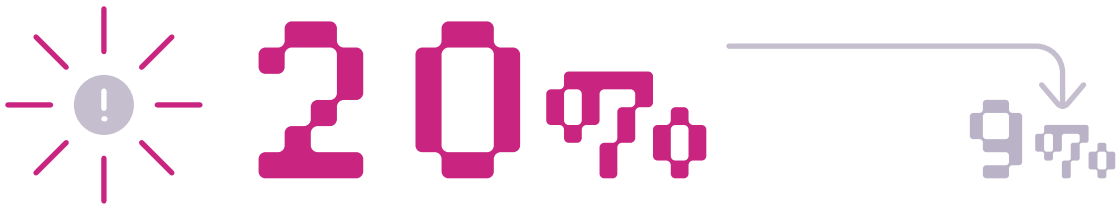
Technology is increasingly becoming a central part of the lives of adolescents. Adolescent boys and girls use technology and online platforms to learn and obtain information and to stay connected with their peers.[71] A study conducted by Plan International with 14,000 girls across 31 countries in all regions found that use of social media is most frequent at a young age (15 years),[72] although other sources reveal that children go online at much younger ages.[73]

Adolescent girls are a growing target group subjected to TFGBV by virtue of their growing engagement in and use of technologies and digital spaces.[74] For example, 80 per cent of images of cases of child sexual abuse materials are of girls aged 11–13 years,[75] and adolescent girls are more often subjected to sexual digital abuse within the context of dating violence.[76] As many as 58 per cent of young women and adolescent girls have been harassed online, according to the study by Plan International, and 85 per cent of those experienced multiple types of TFGBV, including abusive and insulting language (59 per cent), body shaming (39 per cent), threats of sexual (39 per cent) and physical violence (21 per cent), sexual harassment (37 per cent) or stalking (32 per cent).[77] Another survey study by the World Wide Web Foundation and the World Association of Girl Guides and Girls Scouts found that 52 per cent of young women and girls have experienced online abuse and that 68 per cent of this has taken place on social media platforms.[78] Although harassment generally starts between the ages of 14 to 16, some girls reported their first TFGBV experience at the age of 8 years. TFGBV against adolescent girls is also intersectional and many of those who have been harassed and who identify as ethnic minority, LGBTQIA+ or as having a disability said they were harassed because of it.[79] Additionally, the use of social media platforms may have an important negative impact on young people's mental health, particularly of adolescent girls.[80]

Women in public and professional life

Women are disproportionately targeted by TFGBV when their professional lives are supported by an online presence. Women human rights defenders, activists, journalists, bloggers, artists and politicians, for example, are groups of professionals and leaders who are disproportionately affected by the perpetration of TFGBV.[81] This is particularly the case when women and women in professional life are vocal about human rights, feminism, racism and other forms of inequality. These groups of women use digital and social media platforms to support their professional lives as part of engaging with the broader public. The same platforms being relied upon to increase the level of public outreach for advocacy are also being utilized by perpetrators to threaten, harass, stalk and promote hate speech.[82] A recent survey conducted by UNESCO working with 901 journalists in 125 countries found that 73 per cent of women journalists had been subjected to online violence, and 20 per cent of women journalists were attacked offline as a direct consequence of such online violence.[83] Similarly, a global study by the Inter-Parliamentary Union shows that 41.8 per cent of women in politics had seen images or comments with sexual, defamatory or humiliating connotations of themselves being disseminated through social media, and 44.4 per cent had received threats of "death, rape, beatings or abduction during their parliamentary term".[84]

Women who use digital platforms for activism and issue-based advocacy are also particularly and disproportionately targeted. As many as 88 per cent of female respondents to a survey conducted in the UK, who use social media regularly to express their feminist ideas, have been subjected to TFGBV, in the form of trolling, flaming, harassment and threats of physical and sexual violence, on Twitter (60 per cent on Facebook and 46 per cent on blogs).[85] Further, age is a protective factor in the commission of TFGBV. As Plan International found, young women and adolescent girls who speak out online about political issues, feminism, race or sexual and reproductive health and rights face considerable backlash. In fact, 47 per cent of respondents to the Plan International survey reported being attacked for their opinions.[86]



20 per cent of BAME LGBTQIA+ people were subjected to TFGBV compared to 9 per cent of white LGBTQIA+ people.

The importance of intersectionality

TFGBV goes beyond misogyny and sexism, and is also rooted in homophobia, transphobia, racism, ableism and other forms of discrimination. Women and individuals with intersecting identity factors are attacked and discriminated against at higher rates and in distinct forms that combine sexist, racist and homophobic language.[87] Women of colour, Indigenous women, women from religious minorities, LGBTQIA+ women and non-binary individuals, and women with disabilities are targeted in unique and compounded ways.[88] Young women and adolescents that are racialized, have a disability and identify as LGBTQA+ are disproportionately targeted by this type of abuse.[89]

Research shows LGBTQIA+ individuals are more likely to be subjected to different forms of TFGBV, including IBA, harassment and hate speech.[90] For example, a study with 332 sexuality and LGBTQ+ activists from around the world found that all trans and intersex respondents had received threats and intimidating comments online, and that LGBTQIA+ respondents are subjected to higher rates of TFGBV than their heterosexual counterparts.[91] In addition, Black, Asian, Minority, Ethnic (BAME) women and girls are subjected to more attacks than white women and girls. A UK study with 5,000 LGBTQIA+ people showed that 20 per cent of BAME LGBTQIA+ people were subjected to TFGBV compared to 9 per cent of white LGBTQIA+ people.[92]

Digital life is real life: The impact of TFGBV

Despite often being perceived as a less serious and less harmful form of GBV, TFGBV can have as serious consequences on the health and lives of women and girls as physical and sexual violence. The *public*, *pervasive*, *repetitive* and *perpetual* nature of TFGBV as well as the continuum of online–offline violence, causes constant fear and insecurity which is compounded by the lack of specialized and accessible response services and the prevailing incorrect perception that TFGBV is not "real".

The multiple and repetitive nature of TFGBV means that most women experience multiple types of abuse and many, who have an online presence for professional purposes or who are activists and human rights defenders, experience it as a routine part of their online lives. TFGBV will likely be experienced as a pattern and course of behaviour rather than a set of individual acts. This also has the effect that legal responses, which often treat each communication as a separate offence, fall short of addressing the longer-term accumulation of harm.[93]

TFGBV often takes place in a continuum in which actions that start in the digital space may lead to offline GBV perpetration and vice versa.[94] For example, TFGBV is often committed in the context of abusive relationships where technology and digital spaces provide an avenue for the continuation of violence despite having no physical proximity to a survivor. A study conducted among university students in the US has shown that of those who experienced IPV, 92.6 per cent also experienced technology-facilitated aggression, demonstrating the continuum of violence across the physical and non-physical spaces.[95] In other instances, intimate partners may use information and communications technology to stalk, monitor, track and surveille women, combined with in-person stalking.[96] For example, in the UK, a small study among 307 survivors of IPV found that 45 per cent of them had been abused via technology during the relationship, and 48 per cent experienced TFGBV after the relationship ended.[97]

Conversely online harassment and threats exacerbate, trigger and drive offline physical and sexual aggressions.[98] For example, a survey in Malawi found that 53.7 per cent of women experienced physical abuse exacerbated by online violence and that 34.3 per cent were physically harmed or injured as a consequence of it.[99] In other cases, sexualized forms of TFGBV such as IBA have led to honour-related violence against women.[100]

Survivors of TFGBV commonly report severe emotional and psychological distress, anxiety, depression, post-traumatic stress disorder and, in extreme cases, suicidal ideation, self-harm or suicide attempts.[101] Amnesty International conducted a study in eight high-income countries and found out that 54 per cent of women who were subjected to TFGBV experienced panic attacks, anxiety or stress.[102] Similarly, a study with 326 women in Southern India revealed that 28 per cent of respondents felt anxious or depressed and 6 per cent had attempted some form of self-harm.[103] Among young women and girls, 42 per cent of them reported mental or emotional stress and lower self-esteem or loss of confidence, according to a recent study by Plan International in 31 countries.[104] Specifically, survivors of IBSA can experience mental health disorders and psychological distress comparable to those experienced by survivors of sexual assault.[105]

Women and girls who have been subjected to sexual forms of TFGBV, namely IBA, describe the experience as having a devastating impact on their lives. They report that their relationships deteriorate, they have constant feelings of isolation, fear, distrust and being unsafe. These experiences are described as being similar in nature and impact as those felt by survivors of sexual violence.[106]

TFGBV also contributes to an increase in both online and offline isolation at a time when support networks are most crucial. That is, women that have been subjected to or have witnessed[107] TFGBV decrease their participation online and their engagement with technology, and they restrict or self-censor their activities in online platforms. While this is particularly concerning in the context of women who rely on their online presence as part of their professional lives, including journalists and politicians, this violence serves to effectively silence all women. The ramifications of this cannot be underestimated.

This, coupled with the psychological and mental health impacts of TFGBV, has important consequences for women's political and social engagement, employment opportunities and access to education and information.[108] For example, globally, 18 per cent of young women and girls who were subjected to TFGBV had subsequently experienced problems at school.[109] In Malawi, 6 per cent of survivors had lost education opportunities due to TFGBV.

Those who experienced IPV, 92.6 per cent also experienced technology-facilitated aggression, demonstrating the continuum of violence across the physical and non-physical spaces.

Women who have been subjected to TFGBV, especially to sexual forms of TFGBV, are often stigmatized and their reputation damaged. As with other forms of GBV, women are often blamed for the violence they experience and the violence is dismissed as not being "real". Indeed, cases have been documented of survivors being fired or expelled from school after their intimate images were distributed without their consent.[110] Women may also be directly targeted with the sole purpose of damaging their reputation to ensure loss of employment. Reputational damage due to TFGBV may lead to important economic loss for women who own a business, particularly in rural areas.[111] In Malawi, 76.1 per cent of women who were subjected to TFGBV experienced some form of income loss, and 12 per cent were unable to get a new job.[112] Globally, 7 per cent of young women and girls who were subjected to TFGBV had problems in finding or keeping a job.[113]

Furthermore, TFGBV has an important impact on women's productivity. In fact, 55 per cent of participants in a study in eight high-income countries reported that TFGBV decreased their ability to focus on everyday tasks. This same study suggested that, when women withdraw and self-censor after having experienced TFGBV, they may lose contacts and employment opportunities.[114] However, the economic harms of TFGBV do not stop there, as survivors often need to assume high costs for legal fees, health care, relocation or having their information or images removed online.[115] They may also experience economic damage due to financial-targeted abuse, or to loss of home and property.[116]

TFGBV is also a major obstacle to women's equal participation in public life, silencing women's voices and limiting their democratic right to representation and participation. Women are targeted for the views, contributions and the content they create through an online presence. Women politicians, activists and journalists are not the only target for perpetrators of TFGBV, but 47 per cent of young women who spoke out politically also faced attacks on the basis of their opinions.[117] Gendered attacks against women in public life not only target women's opinions, but they tend to be sexual in nature and refer to women's physical appearance and personal life.[118] This silencing of women in the digital space is an attack against their freedom of expression and it has important impacts on women's presence in discussion forums and decision-making spaces, and in their willingness to take leadership roles, thus further reinforcing patriarchal roles and structures.[119]

The impacts of TFGBV are not only personal. There are also significant systemic and structural repercussions. Lower participation of women in the digital space not only widens the gender digital divide, but it also reinforces gender inequality and patriarchal power structures and gender norms.[120] Given the increasing prevalence and use of online and digital spaces and technology to access services, employment and education, it serves as a barrier for women in all their diversity from realizing their human rights. As such, the prevalence of TFGBV is of crisis proportions and will serve as a major barrier to sustainable development and the movement towards gender equality.[121]

Profiling perpetrators of TFGBV

TFGBV can be a tool of IPV or dating violence, but is also perpetrated by acquaintances, work colleagues and strangers, including both individuals or organizations (i.e. for political interests, based on ideology) under the permissiveness, and sometimes complicity, of social media platforms and technology companies.[122]

Technology has also provided opportunities for anonymous and group perpetration of violence to be committed with relative impunity.

The affordability and accessibility of technology to perpetrators is taking IPV into new spaces. Available evidence suggests that most TFGBV is perpetrated by current or previous intimate partners. For example, an Australian study with GBV service providers found that former intimate partners, current intimate partners and date, short-term or casual sexual acquaintances were the most common perpetrators of TFGBV.[123]

Intimate partners or ex-intimate partners

In the context of TFGBV, IPV is often used to intimidate, coerce and maintain control over survivors in order to maintain a relationship or as a punishment or revenge for having left them, as well as a platform to incite others to harm them or to interfere with legal proceedings, among other reasons.[124] Abusive intimate partners stalk, monitor and threaten survivors through location-based services, social media and spyware that is readily available on official app stores – some of which is even advertised to abusers as tools to "Catching Cheating Spouses".[125] Abusive intimate partners may restrict or impede survivors' access to their mobile phones and technology devices, limiting their ability to communicate with others and to seek help. Perpetrators often have access to the survivor's accounts and social circles, thereby easily gaining illicit access to survivors' devices and accounts, including email and social media accounts, and banking information. Having access to these private data may allow perpetrators to install spyware, to track and monitor survivors' location and technology use, to steal or delete survivors' information and to impersonate the survivor.

They may also threaten and blackmail the survivor to reveal intimate photos or private information, and harass the survivor and their social circles through different digital means.[126]

Intimate partners are often able to continue with the abuse even after the relationship ends.[127] In fact, a small study in the UK with 307 women who have been subjected to IPV, 45 per cent of them had also been subjected to TFGBV during the relationship and 48 per cent experienced TFGBV after the relationship ended.[128]

State actors

The State can also be a perpetrator of TFGBV. State actors have the potential to access large amounts of detailed information about survivors including online health data, for example, which contains highly sensitive and confidential information because data are routinely collected in health records and information management systems. State actors also generally have a high level of capacity to surveille, stalk, track and obtain data on individuals to perpetrate violence, the consequences of which may have gendered implications. State actors may use technology and data to perpetrate violence against, for example, activists, women advocates, journalists, gender non-conforming individuals, sexual minorities or rival female political leaders.[129] Furthermore, Governments have the capacity to block access to information and services for sexual and reproductive health, such as online abortion and emergency contraception services.

Although GBV Information Management Systems[130] apply the highest possible standards of robust and ethical data collection and storage to ensure confidentiality of survivor information, cybersecurity and misuse of technology and information by State and other actors, including non-State parties to a conflict remains a risk. Many countries have "inadequate capacity to effectively implement secure information systems; weak or non-existent legal frameworks for data protection; and lack of a dedicated unit in Ministries of Health, with appropriately skilled staff, to oversee data ethics".[131]

Strangers and trolls

As society is becoming increasingly digital, new forms of socializing and engaging with new people and strangers have emerged. Traditional forms of harassment in physical public spaces have moved to the online sphere, allowing perpetrators to easily identify and target women and girls on social media platforms, websites and apps while remaining anonymous.[132]

Trolls are usually strangers who deliberately post comments or messages, upload images or videos and create hashtags for the purpose of annoying, provoking or inciting violence against women and girls for the purpose of their own amusement.[133] Strangers and trolls have been perpetrators of TFGBV since the beginning of the Internet: misogynistic and sexist comments, rape threats and defamatory information have been reported since the early 2000s (i.e. AutoAdmit), with recent cases of increased radicalization and organized harassment campaigns against women (i.e. GamerGate).

A study by Plan International across 31 countries in all regions found that strangers are the most common perpetrators of TFGBV against young women and girls (36 per cent), followed by anonymous social media users (32 per cent) and acquaintances on social media (29 per cent). It is worth noting that 16 per cent of online abuse against young women and girls is perpetrated by groups of strangers.[134]

Harassment from strangers is reported as being more frightening and difficult to stop, and it tends to come from men, who are particularly enraged when women and girls express their opinions and do not conform to traditional norms and ideas of femininity.[135] Among older women, 59 per cent of women who experienced abuse or harassment on Twitter said they were attacked by strangers.[136]

Accountability

Accountability to survivors of TFGBV is perhaps one of the most challenging areas to address. Not only are technologies and digital spaces always changing, but perpetrators may be anonymous and jurisdictions difficult to legislate across.

State responsibility

States hold the responsibility to develop legislative, policy and regulatory frameworks to address TFGBV in order to ensure perpetrator accountability but also to ensure the safety of online platforms, digital spaces and the use of technology. However, current legal frameworks and policies rarely consider TFGBV within existing laws and policies that address GBV and, while some countries may have laws and policies for online safeguarding and security, they are often generic and genderblind, and they fail to take appropriate action to stop digital harm.[137] These frameworks are often insufficient and fail to keep up with emerging technologies, online platforms and other means through which new forms of GBV are perpetrated and amplified. According to the Economist Intelligence Unit, "In 64 of 86 countries, law enforcement agencies and courts appear to be failing to take appropriate corrective actions to address online violence against women."[138] This evidence highlights an important structural gap leaving accountability mechanisms to the goodwill of private technology companies.

Certain forms of TFGBV are legislated against and often criminalized, particularly those that meet definitions of pre-existing criminal offences or cause of civil action. For example, some forms of IBSA, acts of impersonation, defamation, threats of violence, stalking and other invasions of privacy are civil and/or criminal offences in some countries.[139] However, other forms of TFGBV, such as non-criminal online harassment, trolling, online mobbing or creating and disseminating non-sexualized *deepfakes*, may be considered "just speech or expression".[140]

Furthermore, where policies and laws exist, these are not uniformly implemented. Reasons for limited implementation include the perception among law enforcement officials that TFGBV is not a serious offence, as well as the internal gender biases and misconceptions, sexism and power dynamics within patriarchal law enforcement and justice systems that reinforces victim blaming. Further, the interpretations of TFGBV may fall short of meeting the elements of existing criminal offences definitions of violence against women or GBV in law. Further, the ability of law enforcement agencies and justice systems to adequately charge and sentence offenders where the identity of the offender or offenders cannot be traced means that online conduct is committed with impunity. Finally, where the offence is committed in a jurisdiction different to that of the survivor, the means of accessing accountability becomes even more unlikely.

Germany has put in place the "Act to Improve

Enforcement of the Law in Social Networks", or Netzwerkdurchsetzungsgesetz (NetzDG). This law requires social media platforms like Twitter, Reddit and Facebook to remove hate speech and other offensive content within 24 hours. Failure to remove banned content can lead to fines of up to €50 million. Social media platforms are therefore complying – for example, by setting up deletion centres to monitor content and enforcing their own community standards to a larger extent. In 2020, the law was amended to require stronger accountability by social media companies, who are now obligated to report harmful content to the German Federal Criminal Police Office to enable criminal prosecution.[141] That said, the success of the NetzDG in reducing hate speech and harmful and violent content is difficult to monitor and evaluate.[142]

In the European Union, the proposed *Digital Services Act* (2020) explicitly recognizes the systemic harms that digital platforms may cause and places greater obligations on large online platforms, to regularly assess and respond to risks that stem from the use of their services.[143]

In Australia, online safety regulation has, and continues to be, an ongoing priority for regulators. Indeed, the *Online Safety Act 2021 (Cth)* (the "Act") which was recently passed in July 2021 will require that online service providers, social media service providers and other designated Internet service providers have the next six months to ensure their policies and procedures are up to date and compliant with Australian laws. Companies captured under the Act must proactively protect Australian end users and have capacity to respond to notices from the Commission on short notice to remove harmful material. In effect, the obligation to maintain safe spaces is clearly placed upon companies. The Act also continues to build support for the independent statutory body, the eSafety Commission (the "Commission") whose key functions are to enforce the Act and administer a complaints system for the following:

- cyberbullying material targeted at an Australian child;
- non-consensual sharing of intimate images;
- cyberabuse material targeted at an Australian adult; and
- an online content scheme.

Of critical importance is that the burden of removal of harmful material is passed from survivor to the regulating body to manage the immediate removal of the offending material directly with the offending company. Further, the Commission works closely with private companies in building safety features into the design of the platforms, creating partnerships to address TFGBV.[144]

Private technology companies

Private technology companies encapsulate a wide range of organizations including, but not limited to the following:[145]

- designated Internet service providers – entities who allow end users to access online materials, and Internet service providers, being those entities who supply Internet carriage services including among others, Google, Safari and Internet Explorer;
- social media service providers – entities who provide services that connect two end users through online means including among others, Facebook, LinkedIn and Instagram;
- electronic service providers – entities who allow end users to communicate with one another (e.g. Outlook and gaming chat services);
- app distribution service providers – entities who provide access to app services including among others, Google (through the Google PlayStore) and Apple (through IOS App Store);
- hosting service providers – entities who enable hosting of stored materials provided on social media services, relevant electronic services or designated Internet services including, among others, Apple and Microsoft each through their provision of cloud services;
- hardware development companies – entities who create, develop and/or maintain technology equipment, physical assets and other tangible items;
- software development companies – entities who create, design, develop and maintain programmes, applications, frameworks or other software components.

These companies are intermediaries in acts of TFGBV and their actions (or inaction) are central to stopping or amplifying violent acts. While many online platforms and technologies were built for "general application", there are some "purpose-built platforms" that were deliberately designed to commit and propagate acts of TFGBV such as IBSA and non-consensual disclosure of intimate images and therefore profit from abusive behaviours.[146] However, even general application platforms contribute to amplifying TFGBV through distinct features and business models that prioritize growth and profit over human rights, maximize user engagement and favour sensationalized content, and allow automation of abuse and anonymity of perpetrators.[147] These platforms often fail to respond to cases of TFGBV and, for example, suspend survivors' accounts instead of removing offending material and holding abusers accountable, or permitting pages that promote misogynistic content while censoring sex-positive and LGBTQIA+-friendly users. Furthermore, technology companies are often resistant to dealing with equality issues and reproduce misogyny, racism and discrimination in their algorithms. For example, commercial AI systems have been demonstrated to have important gender and skin-type biases,[148] which is likely to stem from a lack of diversity within the technology sector. Products and services that are based on algorithms and AI perpetuate existing implicit biases in society and may result in further discrimination, as they build on available data and information and may themselves be founded from biased assumptions.[149]

Without clear regulation, there is little obligation upon private technology companies to address TFGBV through the removal of harmful content or built-in safety features as part of the platform or technology.

Obligations to promote and protect the safety of end users are critical if TFGBV is to be addressed effectively. While many companies, particularly social media platforms, have introduced content moderation to identify and eliminate abusive content, the design and application of these measures has not always been successful and has placed an additional burden on survivors and individual users to stop the abuse. Furthermore, these mechanisms rely on policies and practices for "freedom of expression" that include many exceptions to what constitutes abuse and hate speech, which are manipulated by perpetrators to silence survivors. Content moderation is also highly selective and inconsistent and decisions are often biased, determined by public opinion, political influence and conflicts of interest, resulting in the removal of innocuous content while abusive content remains unchallenged.[150]

Although content moderation is a first step in stopping TFGBV, more needs to be done by technology and platform companies to ensure safety in technology and online platform use. Technology companies need to collaborate with Governments and civil society in putting mechanisms in place that effectively respond and prevent TFGBV in a gender-responsive and culturally-sensitive manner, while being transparent and proactive in addressing TFGBV from the design of their products to reporting of cases and management of their data.

1 United Nations Department of Economic and Social Affairs (2020). Shaping the Trends of Our Time. Report of the UN Economist Network for the UN 75th Anniversary. Available at: https://www.un-ilibrary.org/content/books/9789210053556

2 Ibid.

3 Flynn, A., Powell, A., and Hindes, S. (2021). Technology-facilitated abuse: a survey of support services stakeholders (Research report, 02/2021). ANROWS. Available at: https://20ian81kynqg-38bl3l3eh8bf-wpengine.netdna-ssl.com/wp-content/uploads/2021/07/4AP.4-Flynn_et_al-TFa_Stakeholder_Survey.pdf UNFPA, UN Women, Quilt.AI (2021). COVID-19 and violence against women: the evidence behind the talk. Available at: https://asiapacific.unfpa.org/en/publications/covid-19-and-violence-against-women-evidence-behind-talk?_ga=2.130256973.39170622.1628523607-1469909938.1607087406 UN Women, UNFPA (2021). Impact of COVID-19 on gender equality and women's empowerment in East and Southern Africa. Available at: https://data.unwomen.org/publications/covid-19-gender-equality-east-and-southern-africa

4 Khoo, C. (2021). Deplatforming misogyny: report on platform liability for technology-facilitated gender-based violence. LEAF. Available at: https://www.leaf.ca/publication/deplatforming-misogyny/

5 Amnesty International (2018). Toxic Twitter. Available at: https://www.amnesty.org/en/latest/news/2018/03/online-violence-against-women-chapter-1/

6 Plan International (2020). Free to Be Online? Girls' and young women's experiences of online harassment. Available at: https://plan-international.org/publications/freetobeonline

7 Ibid.

8 Khoo, Deplatforming Misogyny.

9 E.L. Backe, P. Lilleston and J. McCleary-Sills, "Networked individuals, gendered violence: a literature review of cyber violence", Violence Gender, vol. 5, No. 3, (2018), pp. 135–145. C. McGlynn, E. Rackley and R. Houghton, "Beyond 'revenge porn': the continuum of image-based sexual abuse", Feminist Legal Studies, vol. 15, (2017), pp. 1–22.

10 United Nations Human Rights Council, 20th Sess., Agenda item 3., U.N. Doc A/HRC/20/L.13 (29 Jun. 2012) United Nations (1948). Universal Declaration of Human Rights. Available at: https://www.un.org/en/about-us/universal-declaration-of-human-rights [accessed 11 November 2021].UN General Assembly (1966). International Covenant on Civil and Political Rights, 16 December 1966, United Nations, Treaty Series, vol. 999, p. 171, available at: https://www.ohchr.org/en/professionalinterest/pages/ccpr.aspx [accessed 11 November 2021].

11 OHCHR (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. Available at https://www.ohchr.org/EN/Issues/Women/SRWomen/Pages/SRWomenIndex.aspx

12 Terminology and definitions that refer to TFGBV are multiple and diverse. See Part 4.

13 See glossary in Part 4 for definitions of technology-related terms.

14 Flavia Fascendini and Kateřina Fialová (2011). Voices from digital spaces: Technology related violence against women. Published by Association for Progressive Communications. Available at: https://www.apc.org/sites/default/files/APCWNSP_MDG3advocacypaper_full_2011_EN_0.pdf

15 L., Sardinha and H.E. Nájera Catalán, "Attitudes towards domestic violence in 49 low- and middle-income countries: A gendered analysis of prevalence and country-level correlates", PloS One, vol. 13, No. 10, (2018), e0206101. https://doi.org/10.1371/journal.pone.0206101

16 J. Bailey, N. Henry and A. Flynn, "Technology-Facilitated Violence and Abuse: International Perspectives and Experiences", in The Emerald International Handbook of Technology Facilitated Violence and Abuse, J. Bailey, A. Flynn and N. Henry, eds. (Bingley, Emerald Publishing Limited, 2021) pp. 1–17. https://doi.org/10.1108/978-1-83982-848-520211001

17 Suzie Dunn and Kristen Thomasen, "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, J. Bailey, A. Flynn and N. Henry, eds. (Bingley, Emerald Publishing Limited, 2021).

18 Webinar: Financial freedom - creating economic security and escaping financial abuse. National Summit on Women's Safety, September 2021. Available at: https://regonsite.eventsair.com/national-summit-on-womens-safety/

19 See Part 3 "Glossary of terms" for a more comprehensive list of forms of TFGBV and their definitions.

20 VAW Learning Network (2013). Technology-related Violence Against Women. Available at: http://www.vawlearningnetwork.ca/our-work/issuebased_newsletters/issue-4/index.html

21 Flynn, Powell, and Hindes, Technology-facilitated abuse.

22 N. Henry and A. Powell, "Technology-facilitated sexual violence: a literature review of empirical research". Trauma, Violence & Abuse, vol. 19, No. 2, (2018), pp. 195–208. https://doi.org/10.1177/1524838016650189

23 Ibid.

24 Flynn, Powell, and Hindes, Technology-facilitated abuse. LGBTQI+ populations are particularly susceptible to online harassment and its harms, especially when it comes to threats and/or acts of public disclosure of their gender identity or sexual orientation that may happen with or without extortion and sextortion: S. Dunn (2020). Technology-Facilitated Gender-Based Violence: An Overview (Waterloo, ON: Centre for International Governance Innovation). Available at: https://apo.org.au/node/309987

25 VAW Learning Network, Technology-related violence against women.

26 Henry and Powell, Technology-facilitated sexual violence.

27 C. Parsons, A. Molnar, J. Dalek, J. Knockel, M. Kenyon, B. Haselton, C. Khoo and R. Deibert (2019) The Predator in Your Pocket: A Multidisciplinary Assessment of the Stalkerware Application Industry. The Citizen Lab. Available at: https://citizenlab.ca/2019/06/the-predator-in-your-pocket-a-multidisciplinary-assessment-of-the-stalkerware-application-industry/

28 Flynn, Powell, and Hindes, Technology-facilitated abuse.

29 McGlynn, C., and Rackley, E., "Image-Based Sexual Abuse", Oxford Journal of Legal Studies, vol. 37, No. 3, (2017), pp. 534–561. https://doi.org/10.1093/ojls/gqw033

30 Flynn, Powell, and Hindes, Technology-facilitated abuse.

31 In 2019, during a popular festival in Spain, a perpetrator installed hidden cameras on a public area with the purpose of recording images of women urinating – men have been removed from the recordings. These images, which showed survivors' faces and sexual organs, were then uploaded to porn websites. More than 80 survivors were identified, including minors. This case has been dismissed in court, showing the limited capacity of judicial systems to respond to cases of TFGBV. However, women activists and survivors have joined a movement to reclaim their rights and have contributed to identifying similar cases in other parts of the country. From El Pais (2021). Revuelta en Galicia contra las cámaras ocultas que denigran a las mujeres. Available at: https://elpais.com/sociedad/2021-04-04/revuelta-en-galicia-contra-las-camaras-ocultas-que-denigran-a-las-mujeres.html

32 Henry and Powell, Technology-facilitated sexual violence. N. Henry, A. Flynn and A. Powell, "Technology-facilitated domestic and sexual violence: a review", Violence Against Women, vol. 26, No. 15–16, (2020), pp. 1828–1854. https://doi.org/10.1177/1077801219875821

33 Ibid.

34 Henry and Powell, Technology-facilitated sexual violence. Henry, Flynn and Powell, Technology-facilitated domestic and sexual violence.

35 Henry, Flynn and Powell, Technology-facilitated domestic and sexual violence.

36 S. Craven, S. Brown and E. Gilchrist, "Sexual grooming of children: review of literature and theoretical considerations", Journal of Sexual Aggression, vol. 12, (2006), pp. 287–299, 10.1080/13552600601069414

37 M.A. Franks, "Sexual harassment 2.0", Maryland Law Review, vol. 71, p. 2012655.

38 J.M. MacAllister, The doxing dilemma: seeking a remedy for the malicious publication of personal information. Fordham Law Review, vol. 85, (2017), pp. 2451–2383.

39 S. Eckert and J. Metzger-Riftkin (2020). Doxxing. The International Encyclopedia of Gender, Media, and Communication. https://doi.org/10.1002/9781119429128.iegmc009

40 D. Douglas, "Doxing: a conceptual analysis", Ethics Information Technology, vol. 18, (2016), pp. 199–210.

41 MacAllister, The doxing dilemma.

42 VAW Learning Network, Technology-related violence against women.

43 N. Henry and A. Powell, "Sexual violence in the digital age: the scope and limits of criminal law", Social & Legal Studies, vol. 25, No. 4, (2016), pp. 397–418. doi:10.1177/0964663915624273

44 Flynn, Powell, and Hindes, Technology-facilitated abuse.

45 Fascendini and Fialová, Voices from digital spaces (see footnote 14).

46 VAW Learning Network, Technology-related violence against women.

47 Fascendini and Fialová, Voices from digital spaces (see footnote 14).

48 APC (2020). How Technology is Being Used to Perpetrate Violence Against Women – And to Fight it. Available at: https://www.apc.org/en/pubs/research/how-technology-being-used-perpetrate-violence-agai

49 Nicki Dell, Karen Levy, Damon McCoy and Thomas Ristenpart (2018). How domestic abusers use smartphones to spy on their partners. Available at: https://www.vox.com/the-big-idea/2018/5/21/17374434/intimate-partner-violence-spyware-domestic-abusers-apple-google Parsons, Molnar, Dalek, Knockel, Kenyon, Haselton, Khoo and Deibert, The predator in your pocket.

50 Save the Children (2021). India: girls in India facing greater online risk of child marriage and trafficking during pandemic. Available at: https://www.savethechildren.net/news/india-girls-india-facing-greater-online-risk-child-marriage-and-trafficking-during-pandemic

51 Gulfer Ulas (2019). Female Radicalisation: Why do Women join ISIS? LSE Middle East Centre. Available at: https://blogs.lse.ac.uk/mec/2019/08/15/female-radicalisation-why-do-women-join-isis/ Lisa Blaker, "The Islamic State's use of online social media", Military Cyber Affairs, vol. 1, No. 1, (2015), p. 4. Available at: https://digitalcommons.usf.edu/cgi/viewcontent.cgi?article=1004&context=mca

52 A. Van der Wilk (2018). Cyber violence and hate speech online against women. Study for the FEEM Committee. Available at: w

53 A. Gurumurthy, A. Vasudevan and N. 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. Available at: https://itforchange.net/sites/default/files/1662/Born-Digital_Born-Free_SynthesisReport.pdf

54 D. Freed, J. Palmer, D.E. Minchala, K. Levy, T. Ristenpart and N Dell, "Digital technologies and intimate partner violence: a qualitative analysis with multiple stakeholders", Proceedings of the ACM on Human-Computer Interaction, vol. 1, (2017), pp. 1–22, https://doi.org/10.1145/3134681

55 D.K. Citron, Hate Crimes in Cyberspace (Cambridge, MA: Harvard University Press, 2014). J. West, Cyber-Violence Against Women (Vancouver, BC: Battered Women's Support Services, 2014). www.bwss.org/wp-content/uploads/2014/05/CyberVAWReport-JessicaWest.pdf

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

57 Dunn, Technology-facilitated gender-based violence: an overview; Although technology and digital tools have been used in humanitarian contexts to support programmes and improve response, they also have the potential to exacerbate conflict and to increase the risk of intended and unintended harm to affected populations. State and non-State actors can misuse technology to perpetrate violence and cause further harm to the population, and practices by humanitarian actors – particularly regarding data protection – may leave vulnerable populations at increased risk. More on: https://blogs.icrc.org/law-and-policy/2019/06/12/digital-risks-populations-armed-conflict-five-key-gaps-humanitarian-sector/

58 UN (2019). United Nations Strategy and Plan of Action on Hate Speech. Available at: https://www.un.org/en/genocideprevention/hate-speech-strategy.shtml

59 Dunn, Technology-facilitated gender-based violence: an overview.

60 Douglas, Doxing: a conceptual analysis. Dunn, Technology-facilitated gender-based violence: an overview.

61 Dunn, Technology-facilitated gender-based violence: an overview.

62 K. Levy and B. Schneier, "Privacy threats in intimate relationships", Journal of Cybersecurity (Oxford), vol. 6, No. 1, (2020), https://doi.org/10.1093/cybsec/tyaa006 D. Freed, J. Palmer, D. Minchala, K. Levy, T. Ristenpart and N. Dell, "'A stalker's paradise': how intimate partner abusers exploit technology", presentation at CHI Conference on Human Factors in Computing Systems 2018.

63 L. Hinson, L. O'Brien-Milne, J. Mueller, V. Bansal, N. Wandera and S. Bankar (2019). Defining and Measuring Technology-facilitated Gender-based Violence (Washington DC: International Center for Research on Women). Available at: http://www.svri.org/sites/default/files/attachments/2019-03-25/ICRW_TFGBVMarketing_Brief_v3_WebReady_0.pdf

64 Countries included are Algeria, Argentina, Australia, Bangladesh, Belgium, Brazil, Canada, Chile, China, Colombia, Egypt, France, Germany, Ghana, Guatemala, India, Indonesia, Italy, Japan, Kazakhstan, Malaysia, Mexico, Morocco, Myanmar, Netherlands, Nigeria, Pakistan, Peru, Philippines, Poland, Romania, Russia, Saudi Arabia, South Africa, South Korea, Spain, Taiwan, Tanzania, Thailand, Turkey, Ukraine, United Kingdom, United States, Venezuela and Vietnam.

65 Economist Intelligence Unit (2021). Measuring the prevalence of online violence against women. Available at: https://onlineviolencewomen.eiu.com/

66 Plan International, Free to be online? (see footnote 6).

67 Ibid.

68 WHO (2021). Global, regional and national estimates for intimate partner violence against women and global and regional estimates for non-partner sexual violence against women. Available at: https://www.who.int/news/item/09-03-2021-devastatingly-pervasive-1-in-3-women-globally-experience-violence

69 M. Duggan (2017). Online Harassment 2017. Pew Research Centre. Available at: https://www.pewresearch.org/internet/2017/07/11/online-harassment-2017/

70 Dunn, Technology-facilitated gender-based violence: an overview.

71 Plan International, Free to be online? (see footnote 6).

72 Ibid.

73 Children's Society, Young Minds (2018). Safety net: cyberbullying's impact on young people's mental health: Inquiry report summary. Available at: https://www.youngminds.org.uk/media/gmvdnzcv/executive-summary-pcr144a_social_media_cyberbullying_inquiry_summary_report.pdf

74 Pew Research Centre (2018). Teens, Social Media and Technology 2018. Available at: https://www.pewresearch.org/internet/2018/05/31/teens-social-media-technology-2018/

75 International Web Foundation (2020). IWF 2020 Annual Report | Face the facts. Available at: https://www.iwf.org.uk/report/iwf-2020-annual-report-face-facts

76 Janine M. Zweig, Meredith Dank, Pamela Lachman and Jennifer Yahner, Technology, Teen Dating Violence and Abuse, and Bullying (Washington DC: Urban Institute, 2013). Available at: https://www.urban.org/sites/default/files/publication/23941/412891-Technology-Teen-Dating-Violence-and-Abuse-and-Bullying.PDF

77 Plan International, Free to be online? (see footnote 6).

78 The World Wide Web Foundation (2020). The online crisis facing women and girls threatens global progress on gender equality. Available at: https://webfoundation.org/2020/03/the-online-crisis-facing-women-and-girls-threatens-global-progress-on-gender-equality/

79 Plan International, Free to be online? (see footnote 6).

80 The Wall Street Journal (2021). The Facebook files: Facebook knows Instagram Is toxic for teen girls, company documents show. By Georgia Wells, Jeff Horwitz and Deepa Seetharaman. Available at: https://www.wsj.com/articles/facebook-knows-instagram-is-toxic-for-teen-girls-company-documents-show-11631620739?mod=hp_lead_pos7&mod=article_inline

81 Amnesty International, Toxic Twitter (see footnote 5).

82 Dunn, Technology-facilitated gender-based violence: an overview (see footnote 24).

83 J. Posetti, N. Shabbir, D. Maynard, K. Bontcheva and N. Aboulez (2021). The chilling: global trends in online violence against women journalists. UNESCO. Available at: https://en.unesco.org/news/unesco-releases-pioneering-discussion-paper-online-violence-against-women-journalists

84 Inter-Parliamentary Union (2016). Sexism, harassment and violence against women parliamentarians

85 R. Lewis, M. Rowe and C. Wiper, "Online abuse of feminists as an emerging form of violence against women and girls", British Journal of Criminology, vol. 57, No. 6, (2017), pp. 1462–1481. https://doi.org/10.1093/bjc/azw073

86 Plan International, Free to be online? (see footnote 6).

87 Dunn, Technology-facilitated gender-based violence: an overview (see footnote 24).

88 Amnesty International, Toxic Twitter (see footnote 5).

89 Plan International, Free to be online? (see footnote 6).

90 Dunn, Technology-facilitated gender-based violence: an overview (see footnote 24).

91 Delfina Schenone Sienra and Mariana Palumbo (2017). EROTICS Global Survey 2017: Sexuality, rights and internet regulations. Association for Progressive Communications. Available at: https://www.apc.org/sites/default/files/Erotics_2_FIND-2.pdf

92 Stonewall (2017). LGBT in Britain – Hate Crime and Discrimination. Available at: https://www.stonewall.org.uk/lgbt-britain-hate-crime-and-discrimination

93 Lewis, Rowe and Wiper, Online abuse of feminists as an emerging form of violence against women.

94 OHCHR (2018). Report of the Special Rapporteur on violence against women (see footnote 11).

95 A. Marganski and L. Melander, "Intimate partner violence victimization in the cyber and real world: examining the extent of cyber aggression experiences and its association with in-person dating violence", Journal of Interpersonal Violence, vol. 33, No. 7, (2018), pp. 1071–1095. https://doi.org/10.1177/0886260515614283

96 Flynn, Powell, and Hindes, Technology-facilitated abuse.

97 Laxton, C. (2014). Virtual World, Real Fear. Women's Aid report into online abuse, harassment and stalking. Available at: https://www.womensaid.org.uk/wp-content/uploads/2015/11/Women_s_Aid_Virtual_World_Real_Fear_Feb_2014-3.pdf

98 Dunn, Technology-facilitated gender-based violence: an overview (see footnote 24).

99 D.F. Malanga (2020). Tackling Gender-based Cyber Violence against Women and Girls in Malawi amidst the COVID-19 Pandemic. Available at: https://africaninternetrights.org/sites/default/files/Donald_Flywell-1.pdf

100 GBV AoR Helpdesk (2021). Learning Series on Technology-Facilitated Gender-Based Violence. Learning Brief 1: Understanding technology-facilitated GBV.

101 Ibid.

102 Amnesty International, Toxic Twitter (see footnote 5).

103 Gurumurthy, Vasudevan and Chami, Born digital, born free? (see footnote 53).

104 Plan International, Free to be online? (see footnote 6).

105 Dunn, Technology-facilitated gender-based violence: an overview (see footnote 24). S. Bates, "Revenge porn and mental health: a qualitative analysis of the mental health effects of revenge porn on female survivors", Feminist Criminology, vol. 12, No. 1, (2017), pp. 22–42. https://doi.org/10.1177/1557085116654565

106 C. McGlynn, E. Rackley, N. Henry, N. Gavey, A. Flynn and A. Powell, "'It's torture for the soul': the harms of image-based sexual abuse", Social and Legal Studies, vol. 30, No. 4, (2021), pp. 541–562.

107 Malanga, Tackling gender-based cyber violence.

108 GBV AoR Helpdesk (2021). Learning Series on Technology-Facilitated Gender-Based Violence. Learning Brief 3: Implications of technology-facilitated GBV and actions for humanitarian agencies, donors and online industries.

109 Plan International, Free to be online? (see footnote 6).

110 Dunn, Technology-facilitated gender-based violence: an overview (see footnote 24).

111 Flynn, Powell and Hindes, Technology-facilitated abuse.

112 Malanga, Tackling gender-based cyber violence.

113 Plan International, Free to be online? (see footnote 6).

114 Amnesty International, Toxic Twitter (see footnote 5).

115 Dunn, Technology-facilitated gender-based violence: an overview (see footnote 24).

116 Malanga, Tackling gender-based cyber violence.

117 Plan International, Free to be online? (see footnote 6).

118 Dunn, Technology-facilitated gender-based violence: an overview (see footnote 24). Plan International, Free to be online? (see footnote 6).

119 GBV AoR Helpdesk, Learning Series on Technology-Facilitated Gender-Based Violence (see footnote 108).

120 Dunn, Technology-facilitated gender-based violence: an overview (see footnote 24).

121 GBV AoR Helpdesk, Learning Series on Technology-Facilitated Gender-Based Violence (see footnote 108).

122 Wall Street Journal, The Facebook files (see footnote 80).

123 Flynn, Powell and Hindes, Technology-facilitated abuse.

124 Ibid.

125 Parsons, Molnar, Dalek, Knockel, Kenyon, Haselton, Khoo and Deibert, The Predator in Your Pocket (see footnote 27).

126 Freed, Palmer, Minchala, Levy, Ristenpart, and Dell, A stalker's paradise (see footnote 62).

127 Freed, Palmer, Minchala, Levy, Ristenpart and Dell, Digital technologies and intimate partner violence (see footnote 54).

128 C. Laxton (2014). Virtual World, Real Fear. Women's Aid report into online abuse, harassment and stalking. Available at: https://www.womensaid.org.uk/wp-content/uploads/2015/11/Women_s_Aid_Virtual_World_Real_Fear_Feb_2014-3.pdf

129 Dunn, Technology-facilitated gender-based violence: an overview (see footnote 24).

130 https://www.gbvims.com/

131 Given the increased digitalization of health service for example, there is an increased risk for privacy and confidentiality issues with data and breaches in data protection. Indeed, WHO have reported that even though 70 per cent of 113 countries surveyed had legislation related to basic privacy rights, only 30 per cent of those countries had legislation on the privacy of electronic health records. Even fewer countries had legal frameworks for electronic health records that addressed more than privacy. A lack of policies and legal frameworks on such topics as data ownership, confidentiality, and security has been identified as a major challenge to scaling up digital health records. From World Health Organization (2012). Legal frameworks for eHealth: based on the findings of the second global survey on eHealth. (Global Observatory for eHealth Series, v.5). Available at: https://www.who.int/goe/publications/legal_framework_web.pdf

132 Alisha C. Salerno-Ferraro, Caroline Erentzen and Regina A. Schuller, "Young women's experiences with technology-facilitated sexual violence from male strangers", Journal of Interpersonal Violence, (2021), https://doi.org/10.1177/08862605211030018

133 eSafety Commission Australia. Online abuse targeting women. Available at: https://www.esafety.gov.au/women/online-abuse-targeting-women

134 Plan International, Free to be online? (see footnote 6).

135 Ibid.

136 Amnesty International, Toxic Twitter (see footnote 5).

137 UNICEF East Asia & Pacific (2021). What we know about the gender digital divide for girls: a literature review. Available at: https://www.unicef.org/eap/reports/innovation-and-technology-gender-equality-0

138 Economist Intelligence Unit, Measuring the prevalence of online violence (see footnote 65).

139 Khoo, Deplatforming misogyny (see footnote 4).

140 Ibid.

141 Oltermann, P. 5 January 2018. Tough new German law puts tech firms and free speech in spotlight. Available at: https://www.theguardian.com/world/2018/jan/05/tough-new-german-law-puts-tech-firms-and-free-speech-in-spotlight

142 Khoo, Deplatforming misogyny (see footnote 4).

143 Ibid.

144 eSafety Commissioner. Available at: https://www.esafety.gov.au/ [accessed 4 Nov 2021].

145 Online Safety Act 2021 (Cth). No. 76, 2021. (Austl.)

146 Khoo, Deplatforming misogyny (see footnote 4).

147 Ibid.

148 Larry Hardesty (2018). Study finds gender and skin-type bias in commercial artificial-intelligence systems. Available at: https://news.mit.edu/2018/study-finds-gender-skin-type-bias-artificial-intelligence-systems-0212

149 Rebecca Heilweill (2020). Why algorithms can be racist and sexist. Available at: https://www.vox.com/recode/2020/2/18/21121286/algorithms-bias-discrimination-facial-recognition-transparency Brian Resnick (2019). Yes, artificial intelligence can be racist. Available at: https://www.vox.com/science-and-health/2019/1/23/18194717/alexandria-ocasio-cortez-ai-bias

150 Khoo, Deplatforming misogyny (see footnote 4).

Part 2

Recommendations and Strategies for TFGBV

Prevention and Response

Given the new and constantly evolving forms and the specific characteristics of TFGBV, prevention and response efforts require the collective efforts of national Government and private technology companies, including platform companies. This must be guided by approaches based on human rights, taking account of the experiences of women and girls in all their diversity to ensure that reform and regulation to prevent and respond to TFGBV is meeting their needs.

Below is a non-exhaustive list of recommendations for States and private technology companies respectively to address the growing prevalence and impact of TFGBV. These recommendations require significant and sustained financial, technical and human resource investment from national and international bodies, Governments and the private sector. They also require strong partnerships between private technology companies, Government, digital rights and feminist movements, GBV service providers, academics and, finally and most importantly, survivors of TFGBV.

1 Recommendations for National Governments

Policy and legislation

Law and policy should be shaped within a human rights framework that addresses the structural discrimination, violence and inequalities that women face. Legal frameworks must adequately protect all women's human rights online, including the right to life free from violence, freedom of expression and access to information, and the right to privacy and data protection.151 As well as strengthening accountability of perpetrators, laws must regulate private technology companies to enforce safety and response mechanisms to prevent and mitigate the occurrence of TFGBV.

Policy and legislation must be developed with the full participation and consultation of survivors of TFGBV, front-line providers and services as well as scholars and substantive experts in the fields of platform regulation, content moderation and algorithmic accountability.

- Recognition and integration of TFGBV across civil, criminal laws, regulations and policies to regulate private technology companies and hold offenders to account.
- Establish an independent statutory body to address TFGBV with a mandate which may include the following: (a) powers to administer legal remedies and support to individuals impacted by TFGBV on digital platforms; (b) regulatory and enforcement powers over private technology companies to integrate safety mechanisms and immediately remove harmful content; (c) progress research on TFGBV to support evidence-based law and policy; (d) advocate for and facilitate removal of harmful content upon reporting of survivors or front-line service providers; (e) provide training and education to the public, relevant stakeholders and professionals; and (f) support partnerships with private technology companies to enable compliance with mandatory or voluntary safety requirements.
- Where new laws and policies are introduced, they are adequately budgeted to ensure implementation and the relevant enforcement authorities and the judiciary are provided with the requisite training and skills accordingly.
- Laws must require the provision of expedient, practical and accessible remedies for those targeted by TFGBV, including support for accessible moderation spaces to appeal refusal to remove offending materials.
- Require strengthened systems to support data security including confidential information collected and managed by the State and data collected through location-based applications and platforms.
- International agreements and a common legislative framework to fight cross-border TFGBV should be put in place. Perpetrators are often not held accountable due to cross-jurisdictional issues, as they commit the abuse from different states or countries.

In the regulation of private technology companies:

- Mandate and enforce laws and regulations that require private technology companies to develop, maintain and implement policies to respond to and mitigate the occurrence of TFGBV through a range of processes including the following: (1) visible, easily accessible, plain-language complaint and abuse reporting mechanisms of harmful content, (2) **immediate** removal of harmful content when reported (while maintaining records for evidentiary purposes); (3) effective moderation mechanisms; (4) require training of all staff to understand their role in monitoring and removal of harmful content relating to TFGBV; and (5) provision of independent audits and publish comprehensive annual transparency reports relating to implementation of the policies.

- Ensure regulation to support the immediate removal of defined harmful content from a platform without a need for recourse to court order, costs and other associated and legal challenges.[152]

- Where an order is provided against a platform company, ensure that it requires the removal of the content from any of that platform's parent, subsidiary or sibling platform companies where the same content also appears.[153]

- Consider the provision of incentives to private technology companies to encourage compliance with and active promotion of the protection of women and girls using their services.

- Advertising, sales and distribution of apps and devices marketed with monitoring purposes must be carefully monitored and only permitted for particular purposes. Access to these must also be restricted including through removal from official app stores.

Strengthened response mechanisms

Sustained and deep investments in survivor-centred and feminist-informed response mechanisms that address all forms of TFGBV, both as an isolated incident and as part of a pattern of behaviour, is critical.

- Ensure participatory and feminist approaches in designing laws, policies, strengthened response mechanisms and associated training materials to capture the breadth of experience of survivors.
- Strengthen survivor-centred and comprehensive response services for TFGBV through the provision of continuous training and capacity-building for service providers across sectors (including law enforcement officials, judiciary, GBV case workers, health care and psychosocial service providers, housing and social service workers) to support safe and survivor-centred identification, response and early intervention of TFGBV.
- Engage professional bodies, including those intended to support journalists and politicians to provide a convening space for collaboration between professional associations and TFGBV response services.
- Ensure the integration of private technology companies into existing referral mechanisms of front-line GBV responders to ensure active and immediate response to TFGBV through a range of mechanisms, including through support for an intermediary service with the capacity to facilitate access of front-line GBV response services to focal points within private technology companies.
- Financial, human and technical resources for front-line support workers and community-based organizations to enable immediate and effective responses with the full support of health, social, policing and legal services including private technology companies.
- Ensure shelters and safe spaces are provided with requisite security (physical and online) to enforce confidentiality of the location.
- Ensure that all actors across the justice system are provided with the training and resources to ensure a high level of expertise and familiarity with information and communications technology and their functioning as well as digital evidence to ensure that the appropriate evidence is collected, preserved and given due weight and to avoid retraumatization of survivors during judicial proceedings.[154]

Investment in prevention

Prevention of TFGBV requires working with individual and groups of survivors, advocates and activists, GBV service providers as well as private companies, public and government departments and organizations as well as professional associations. A critical strategy and approach in supporting and maintaining prevention efforts will be through the convening role of national Government to create and sustain these partnerships.

Education

- Investment to improve digital literacy among adolescents, women, particularly older women, activists and professionals in all their diversity, through the provision of free accessible courses or workshops that can be integrated into school, university and vocational learning institutions, workplaces and community spaces.
- Integration of modules and concepts into curricula and training packages (including comprehensive sexuality education) to support healthy online behaviour and interactions.[155]
- Development of accessible curricula and training for education facilities and community services to provide training for members of the community of all ages and in all their diversity.
- Provide access to support services for community members and in particular women in all their diversity in navigating technology and online spaces.
- Development of tools to support women in all their diversity, parents and educators to enable them to protect the online privacy of children and students.
- Continued and scaled up work to ensure GBV prevention programmes that include engagement with men and boys in transforming harmful masculinities to address online behaviours.
- Investment in evaluations of education and prevention programmes to determine effectiveness in changing attitudes and behaviours online.

Support community action and advocacy

- Promote the creation of spaces for peer groups vulnerable to TFGBV as an essential support network. Examples of successful peer support groups include those led by women journalists.[156]
- Promote and protect women's voices and safe participation in the online sphere, through promoting supportive behaviours and providing women and girls with the necessary skills to counteract abuse.
- Actively support feminist advocates and activists, women human rights defenders, journalists and politicians who maintain an online presence to continue to engage with the public through this medium without fear of TFGBV through creation of peer networks (where there are not already) and facilitating proactive content moderation of private technology companies.

Data security

- Dedicated resources to develop and implement law, policies, systems and processes as well as capacitated staff to ensure confidential data security.
- Resources to enable front-line services providers to continue to safely collect and protect data relating to survivors of GBV. This is critical given the offline and online continuum of violence, particularly in the context of IPV.

Data and research

Strengthened data and research are required to provide a foundation upon which policies, programmes, laws and advocacy strategies can be developed. It is critical to understand the forms of TFGBV, its impacts, primary targets and perpetrators as well as the remedies that are needed and wanted, and appropriate accountability mechanisms.

- Global and standardized definitions and terminology of TFGBV and its different forms, tactics and associated behaviours need to be developed and agreed upon.
- Inclusion of TFGBV as a form or experience of violence to be included in population-based standardized surveys[157] including, for example, the WHO Multi-Country Study Methodology or the Demographic Health Survey which are used to determine the prevalence of GBV. For this, standardized measures of TFGBV, including all its forms, need to be developed, tested and adapted across contexts and cultures.
- Ensure inclusion of TFGBV as a form of violence in GBV administrative data systems. This may require, for example, amendment of intake forms and case management documentation to record the context (online or offline) within which the violence took place. This will provide a strengthened understanding of how cases of TFGBV are being reported, referred and managed as well as an analysis of trends, all of which can inform evidence-based advocacy and interventions.
- Increased attention and focus on the generation of research to determine "what works" to prevent and respond to TFGBV.
- Resource in-depth empirical, interdisciplinary and law and policy research by TFGBV scholars, TFGBV experts and community-based organizations on TFGBV and the impacts of emerging technologies on those subjected to TFGBV across all ages and intersectionalities. For example, supporting research to prevent abuse in encrypted communication.[158]

GOVERNO DO DISTRITO DE CHICUALACUALA

SERVIÇO DISTRITAL DE SAÚDE, MULHER E ACÇÃO SOCIAL

PROGRAMA DE VIOLÊNCIA BASEADA NO GÊNERO

Nº DE ORDEM	DATAS	ACTIVIDADE	RESPONSABILIDADE
01	01/12/20	Realização de palestras de sensibilização e conaciencialização sobre a Violência Baseada no Género	Ponto focal de VBG
02	08/12/20	Encontro de Coordenação Multisectorial de Atendimento Integrado a Violência Baseada no Género	Mecanismo Multissectorial
03	15/12/20	Realização de Supervisão e Apoio Técnico	Ponto focal de VBG
04	22/12/20	Sessões de debates radiofónicos sobre a Violência Baseada no Género	Ponto focal de VBG
05	29/12/20	Realização de visitas domiciliares a famílias vítimas de Violência Baseada no Género	Ponto focal de VBG

Chicualacuala, 07 de Dezembro de 2020

Salomão Gonçalves Matavele

/Tec. Sup. de Saúde N1/

LINHAS DE DENÚN

86 274 33 94-

87 542 43 68-

86 872 10 91-

2 Recommendations for Private Technology Companies

Private companies must recognize their role in the perpetration of TFGBV and create and nurture long-term and productive partnerships with GBV service providers, women in all their diversity, professional associations, scholars and national Government to support informed, effective and immediate safety mechanisms which immediately respond, protect and promote women and girls' right to be free from violence both online and offline.

- Development and application of technologies and digital platforms must be in partnership and with the participation of women in all their diversity as well as organizations and advocates,[159] to ensure relevant and accessible safety features and complaint mechanisms.
- Prevention, mitigation and response to TFGBV must be included in the Standard Operating Procedures of social media and technological companies to ensure immediate removal of harmful content, active moderation and TFGBV mitigation measures.
- Complaints mechanisms must ensure an **immediate** response and removal of harmful material, pending further investigation in accordance with best practice policies as well as removal of the material from all subsidiary and associated sites.
- Ensure clear and transparent content moderation policies and responses.
- Safety must be incorporated at the design stage. For practical guidance and actionable recommendations, see the outcomes and recommendations report "Tech Policy Design Lab: Online Gender-Based Violence and Abuse", which builds on the results from a series of workshops with relevant stakeholders, including survivors of TFGBV and technology companies.[160]
- Focal points designated within the company, available at all times, to support complaints and remove offensive and violating material.
- Require all staff of startup technology companies and platforms to participate in training to increase understanding of TFGBV and their role in monitoring and removal of harmful content.

151 Michael Geist (2021). Tracking the submissions: what the government heard in its online harms consultation (since it refuses to post them). Available at: https://www.michaelgeist.ca/2021/10/tracking-the-submissions-what-the-government-heard-in-its-online-harms-consultation-since-it-refuses-to-post-them/

152 H. Young and E. Laidlaw (2020). Creating a Revenge Porn Tort for Canada. Supreme Court Law Review, 2020, Available at SSRN: https://ssrn.com/abstract=3586056

153 Khoo, Deplatforming misogyny (see footnote 4).

154 S. Dunn and M. Aikenhead, "On the internet, nobody knows you are a dog: contested authorship of digital evidence in cases of gender-based violence", Canadian Journal of Law and Tech. (forthcoming).

155 UNFPA (2021). Comprehensive Sexuality Education as a GBV prevention strategy.

156 GBV AoR Helpdesk (2021). Learning Series on Technology-Facilitated Gender-Based Violence. Learning Brief 2: Strategies and actions for preventing and responding to technology-facilitated GBV.

157 https://asiapacific.unfpa.org/sites/default/files/pub-pdf/kNOwVAWdata%20Methodology.pdf

158 Cornell Tech (2021). New project aims to prevent abuse in encrypted communication. Available at: https://tech.cornell.edu/news/preventing_abuse_in_encrypted_communication/

159 Organizations and advocates such as the Association for Progressive Communications (https://www.apc.org/en), the World Wide Web Foundation (https://webfoundation.org/), Derechos Digitales (https://www.derechosdigitales.org/), Internet Democracy Project (https://internetdemocracy.in/) or Gender IT (https://genderit.org/es).

160 See World Wide Web Foundation, Feminist Internet and Craig Walker (2021). Tech Policy Design Lab: Online Gender-Based Violence and Abuse. Available at: https://uploads-ssl.webflow.com/61557f76c8a63ae527a819e6/61557f76c8a63a65a6a81adc_OGBV_Report_June2021.pdf

Part 3

Snapshot of Surveys

to Measure Prevalence of TFGBV

The table below provides a snapshot of the range of prevalence studies that have been published relating to TFGBV.

Source	Location	Term used and definition	Population and sample size	Prevalence data
Economist Intelligence Unit (2021)[161]	51 countries with the highest Internet penetration rates across all regions	Online violence against women – women who reported personal experiences with online violence	4,500 women aged 18–74 years	38%
African Development Bank Group (2016)[162]	Kenya	Online harassment Contacted by imposters online, personal hate speech, cyberbullying and trolling while online	Not defined	>33% (online harassment) 33% (other forms of violence, including hate speech, cyberbullying and trolling)
Plan International (2020)[163]	31 countries across all regions	Online harassment, "rangingfrom threats of physical or sexual violence to racist comments and stalking"	14,000 young women and girls aged 15–25 years	58%
The World Wide Web Foundation (2020)[164]	180 countries	Online abuse, including threatening messages, sexual harassment and the sharing of private photos and videos without permission	8,109 respondents (51% women), mostly 15–30 years of age	52% (of women)
Neema Iyer, Bonnita Nyamwire and Sandra Nabulega (2020)[165]	Five African countries (Ethiopia, Kenya, Uganda, Senegal and South Africa)	Online GBV, including sexual harassment, offensive name calling, stalking and doxxing	3,306 women aged 18–65 years, that access and use the Internet at least once a week	28.2%
Digital Rights Foundation (2017)[166]	Pakistan	Stalking or harassment via messaging apps	1,400 young women students (18 or older) and their female teachers at 17 universities across Pakistan	40%

Source	Location	Term used and definition	Population and sample size	Prevalence data
F.M. Hassan, F.N. Khalifa, E.D. El Desouky et al. (2020)[167]	Egypt	Cyberviolence against women and girls	356 adult females (≥18 years old) present on women's Facebook groups	41.6%
D. Woodlock, K. Bentley, D. Schulze, N. Mahoney, D. Chung and A. Pracilio (2020)[168]	Australia	Technology-facilitated stalking and abuse	442 domestic, family and sexual violence practitioners (426 women)	99.3% (of participants have worked with clients subjected to technology-facilitated abuse)

The prevalence of specific forms of TFGBV have also been captured in regional and national data-collection efforts, a summary of which is highlighted in the table below:

Form of TFGBV	Subtype	Location and population	Prevalence or data snapshot	Source
Online harassment	**Online harassment, after the age of 15 years**	European Union, women	11%	A. Van der Wilk (2018)[169]
		31 countries worldwide, young women and girls aged 15–25 years	58%	Plan International (2020)[170]
	Online harassment, abusive and insulting language	31 countries worldwide, young women and girls aged 15–25 years	59%	Plan International (2020)[171]
	Online harassment, threats of sexual violence	31 countries worldwide, young women and girls aged 15–25 years	39%	Plan International (2020)[172]
	Online harassment, threats of physical violence	31 countries worldwide, young women and girls aged 15–25 years	21%	Plan International (2020)[173]
Sexualized forms of online abuse		United States, men and women	9% of men and 21% of women 18–29 years (i.e. more than double)	Pew Research Centre (2017)[174]
		Canada, undergraduate students, mean age 23.79 years and 72% female	88% of women	Lindsey A. Snaychuk and Melanie L. O'Neill (2020)[175]
		31 countries worldwide, young women and girls aged 15–25 years	37%	Plan International (2020)[176]

Form of TFGBV	Subtype	Location and population	Prevalence or data snapshot	Source
Cyberstalking	**Cyberstalking, after the age of 15 years**	European Union, women	5%	A. Van der Wilk (2018)[177]
	Cyberstalking, in the past year	European Union, women	2%	A. Van der Wilk (2018)[178]
		31 countries worldwide, young women and girls aged 15–25	32%	Plan International (2020)[179]
		Senegal, South Africa, Kenya, Uganda and Ethiopia, women 18–65	26.7%	N. Iyer, B. Nyamwire and S. Nabulega (2020)[180]
Image-based sexual abuse	**Non-consensual sharing of nude or sexual images**	High-income countries (review study)	1–12%	N. Henry, A. Flynn and A. Powell (2020)[181]
	Threats to share nude or sexual images	High-income countries (review study)	1–15%	N. Henry, A. Flynn and A. Powell (2020)[182]
	Overall prevalence, estimate	Systematic review and meta-analysis, mainly Western populations	9%	U. Patel and R. Roesch (2020)[183]
Technology-facilitated unwanted sexual experiences	**Being asked to engage in unwanted sexual activities or behaviours**	The Netherlands, adults aged 18–88 years	4.6% of men, 6.7% of women	S.E. Baumgartner, P.M. Valkenburg and J. Peter (2010)[184]
	Engage in at least 1 out of 10 sexual victimization behaviours	Spain, adults	38%	M. Gámez-Guadix, C. Almendros, E. Borrajo and E. Calvete (2015)[185]
Doxxing		United States	29%	Amnesty International (2018)[186]
		Eight high-income countries	11%	Amnesty International (2018)[187]

Form of TFGBV	Subtype	Location and population	Prevalence or data snapshot	Source
TFGBV directly related to trafficking or for the purpose of recruitment and exploitation		Serbia, survivors of human trafficking	31%	Andrijana Radoičić (2020)[188]
Impersonation	**At least one impersonation threat**	India, Bangladesh and Pakistan, cisgender and non-cisgender members	15%	N. Sambasivan, A. Batool, N. Ahmed, T. Matthews, K. Thomas, L.S. Gaytán-Lugo, D. Nemer, E. Bursztein, E. Churchill and S. Consolvo (2019)[189]
	Impersonation attacks involving the creation of false profiles with the survivor's identity	India, Bangladesh and Pakistan, cisgender and non-cisgender members	12%	N. Sambasivan, A. Batool, N. Ahmed, T. Matthews, K. Thomas, L.S. Gaytán-Lugo, D. Nemer, E. Bursztein, E. Churchill and S. Consolvo (2019)[190]
Gendered hate speech		European Union	3.1% of reports to Internet platforms involve gender hate speech	A. Van der Wilk (2018)[191]
		Malawi, women 15–45 years	46.3%	D.F. Malanga (2020)[192]
Defamation		United States, adult men and women	26% of adults have had false information about them being posted online, the gender differences are modest	Pew Research Centre (2017)[193]
		Malawi, women 15–45 years	43.3%	D.F. Malanga (2020)[194]

161 Economist Intelligence Unit, Measuring the prevalence of online violence (see footnote 65).

162 African Development Bank Group (2016). Minding the gaps: identifying strategies to address gender-based cyberviolence in Kenya. Available at: https://www.afdb.org/fileadmin/uploads/afdb/Documents/Generic-Documents/Policy_Brief_on_Gender_Based_Cyber_Violence_in_Kenya.pdf

163 Plan International, Free to be online? (see footnote 6).

164 The World Wide Web Foundation, The online crisis facing women and girls (see footnote 78).

165 N. Iyer, B. Nyamwire and S. Nabulega (2020) Alternate Realities, Alternate Internets: African Feminist Research for a Feminist Internet, Pollicy. Available at: https://ogbv.pollicy.org/report.pdf

166 Digital Rights Foundation (2017). Measuring Pakistan Women's Experiences of Online Violence. Available at https://digitalrightsfoundation.pk/wp-content/uploads/2017/05/ Hamara-Internet-Online-Harassment-Report.pdf

167 F.M. Hassan, F.N. Khalifa, E.D. El Desouky, M.R. Salem and M.M. Ali, "Cyber violence pattern and related factors: online survey of females in Egypt", Egyptian Journal of Forensic Sciences, vol. 10, No. 6, (2020), https://doi.org/10.1186/s41935-020-0180-0

168 D. Woodlock, K. Bentley, D. Schulze, N. Mahoney, D. Chung and A. Pracilio, (2020). Second National Survey of Technology Abuse and Domestic Violence in Australia. WESNET. Available at: https://wesnet.org.au/about/research/2ndnatsurvey/

169 Van der Wilk, Cyber violence and hate speech online against women (see footnote 52).

170 Plan International, Free to be online? (see footnote 6).

171 Ibid.

172 Ibid.

173 Ibid.

174 Duggan, Online harassment 2017 (see footnote 69).

175 Lindsey A. Snaychuk and Melanie L. O'Neill, "Technology-facilitated sexual violence: prevalence, risk, and resiliency in undergraduate students", Journal of Aggression, Maltreatment & Trauma, vol. 29, No. 8, (2020), pp. 984–999, DOI: 10.1080/10926771.2019.1710636

176 Plan International, Free to be online? (see footnote 6).

177 Van der Wilk, Cyber violence and hate speech online against women (see footnote 52).

178 Ibid.

179 Plan International, Free to be online? (see footnote 6).

180 Iyer, Nyamwire and Nabulega, Alternate realities, alternate internets (see footnote 165).

181 Henry, Flynn and Powell, Technology-facilitated domestic and sexual violence (see footnote 32).

182 Ibid.

183 U. Patel and R. Roesch, "The prevalence of technology-facilitated sexual violence: a meta-analysis and systematic review", Trauma, Violence, & Abuse, (2020), doi:10.1177/1524838020958057

184 S.E. Baumgartner, P.M. Valkenburg and J. Peter, "Unwanted online sexual solicitation and risky sexual online behavior across the lifespan", Journal of Applied Developmental Psychology, vol. 31, (2010), pp. 439–447.

185 M. Gámez-Guadix, C. Almendros, E. Borrajo and E. Calvete, "Prevalence and association of sexting and online sexual victimization among Spanish adults", Sexuality Research and Social Policy, vol. 12, (2015), pp. 145–154.

186 Amnesty International, Toxic Twitter (see footnote 5).

187 Ibid.

188 Andrijana Radoičić (2020). Behind the screens: Analysis of human trafficking victims abuse in digital surroundings. Available at: http://www.atina.org.rs/en/behind-screens-analysis-human-trafficking-victims-abuse-digital-surroundings

189 N. Sambasivan, A. Batool, N. Ahmed, T. Matthews, K. Thomas, LS. Gaytán-Lugo, D. Nemer, E. Bursztein, E. Churchill and S. Consolvo, "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, 4–9 May 2019. Available at: https://storage.googleapis.com/pub-tools-public-publication-data/pdf/acf12158ab313c1e9d80b87ede-065254f64ad9a7.pdf

190 Ibid.

191 Van der Wilk, Cyber violence and hate speech online against women (see footnote 52).

192 Malanga, Tackling gender-based cyber violence (see footnote 99).

193 Duggan, Online harassment 2017 (see footnote 69).

194 Malanga, Tackling gender-based cyber violence (see footnote 99).

Part 4

Glossary of Terms

Definitions of TFGBV

Source	Term	Definition
OHCHR (A/HRC/38/47, para. 23)[195]	**GBV against women online**	GBV against women online, and especially against women journalists who use information and communications technology as tools for their work, includes any act of violence that is committed, assisted or aggravated in part or fully by the use of information and communications technology, such as mobile phones and smartphones, the Internet, social media platforms or email, against a woman because she is a woman, or that affects women disproportionately.
A. Flynn, A. Powell and S. Hindes (2021)[196]	**Technology-facilitated abuse (TFA)**	TFA encompasses existing patterns of violence, harassment and abuse that are extended and amplified by digital media, as well as new forms of abuse, such as IBA. TFA is wide-ranging and inclusive of many subtypes of interpersonal violence and abuse utilizing mobile, online and other digital technologies. These can include stalking and monitoring behaviours, psychological and emotional abuse (including threats), sexual violence and IBA, as well as sexual harassment. The term also sometimes refers more broadly to forms of general online harassment and cyberbullying. TFA is characterized by an intersection of gender power relations and sexually based and/or intimate partner harms, as it may imply a digital extension of coercive control behaviours employed by perpetrators of family violence to monitor, threaten and restrict partners or ex-partners. TFA is further understood to frequently target and disproportionately impact women.
United Nations[197]	**Online and information and communications technology-facilitated violence against women and girls**	The definition of online violence against women extends to any act of GBV against women that is committed, assisted or aggravated in part or fully by the use of information and communications technology, such as mobile phones and smartphones, the Internet, social media platforms or email, against a woman because she is a woman, or affects women disproportionately.
European Institute for Gender Equality[198]	**Cyberviolence against women and girls**	GBV that is perpetrated through electronic communication and the Internet. Although cyberviolence can affect both women and men, women and girls experience different and more traumatic forms of cyberviolence. There are various forms of cyberviolence against women and girls, including, but not limited to, cyberstalking, non-consensual pornography (or "revenge porn"), gender-based slurs, hate speech and harassment, "slut-shaming", unsolicited pornography, "sextortion", rape threats and death threats, and electronically facilitated trafficking. Cyberviolence is not a separate phenomenon to "real world" violence, as it often follows the same patterns as offline violence.

Source	Term	Definition
International Centre for Research on Women[199]	**Technology-facilitated Gender-based violence**	TFGBV is action by one or more people that harms others based on their sexual or gender identity or by enforcing harmful gender norms. This action is carried out using the Internet and/or mobile technology and includes stalking, bullying, sexual harassment, defamation, hate speech and exploitation.
TEDIC[200]	**Digital Gender Violence**	Digital (or online) gender violence refers to acts of gender violence committed, instigated or aggravated, in part or totally, through the use of information and communications technology, social media platforms or email services. Such violence causes psychological and emotional damage, reinforces prejudice, damages the reputation, causes economic loss, poses barriers to participation in public life, and it may lead to sexual violence and other forms of physical violence.
A. Powell, A.J. Scott and N. Henry (2018)[201]	**Digital harassment and abuse**	Umbrella term that refers to a range of harmful interpersonal behaviours experienced via the Internet, as well as via cellular phone and other electronic communication devices. These online behaviours include offensive comments and name calling, targeted harassment, verbal abuse and threats, as well as sexual, sexuality and gender-based harassment and abuse. Sexual, sexuality and gender-based harassment and abuse refers to harmful and unwanted behaviours either of a sexual nature, or directed at a person on the basis of their sexuality or gender identity.
Association for Progressive Communications' Women's Rights Programme[202]	**Technology- related violence against women**	Acts of gender-based violence that are committed, abetted or aggravated, in part or fully, by the use of information and communications technology, such as mobile phones, the Internet, social media platforms and email.
J. Bailey, A. Flynn and N. Henry[203]	**Technology-facilitated violence and abuse**	Umbrella term used to describe the use of digital technologies to perpetrate interpersonal harassment, abuse and violence, such as sexual violence, domestic and family violence, prejudice-based hatred and online othering.

Forms of TFGBV and definitions

A

Astroturfing
Dissemination or amplification of content (including abuse) that appears to arise organically at the grass-roots level and spread, but is actually coordinated (often using multiple fake accounts) by an individual, interest group, political party or organization.[204]

C

Catfishing
Internet scam where the abuser pretends to be someone they are not, by creating false online identities in social media – often using other people's photos and developing extensive fake life stories and experiences, jobs and friends – with the objective of seducing another person or making them believe they are in an online relationship and use this as a means to ask for money, gifts or intimate images.[205]

Cross-platform harassment
Coordinated and deliberately deployed harassment against a target, by a single harasser or a group of harassers, across multiple online spaces, social media and communication platforms, taking advantage of the fact that most platforms only moderate content on their own sites.[206]

Cyberbullying
Umbrella term that refers to a "wilful and repeated harm inflicted through the use of computers, cell phones and other electronic devices",[207] usually using textual or graphical content and with the aim of frightening and undermining someone's self-esteem or reputation.[208] This term is mainly used in relation to children and young people.[209]

Cyberflashing
Form of image-based abuse whereby a person sends an unsolicited image of their genitals or sexually explicit materials to another person without their consent.[210] Also referred to as "dick pics", cyberflashing is a form of unsolicited pornography which refers more widely to "sending unsolicited pornography, violent rape porn gifs or photographs in which a target's photograph has been sexualized".[211]

Cyberstalking
Severe form of cyberobsessional pursuit, motivated by relational control or destruction, that consists of the use of technology to repeatedly stalk and monitor someone's activities and behaviours in real-time or historically and that causes the survivor to feel fear.[212]

Cyberobsessional pursuit
Unwanted pursuit of intimacy through a repeated invasion of a person's sense of physical or symbolic intimacy, using digital or online means.[213]

D

Deadnaming
A form of direct harassment in which a target's former name is revealed against their wishes for the purposes of harm. This technique is most commonly used to out members of the LGTBQIA+ community who may have changed their birth names for any variety of reasons, including to avoid professional discrimination and physical danger.[214]

Deepfakes
Digital images and audio that are artificially altered or manipulated by AI and/or deep learning to make someone appear to do or say something he or she did not actually do or say. Pictures or videos can be edited to put someone in a compromising position or to have someone make a controversial statement, even though the person did not actually do or say what is shown. Increasingly, it is becoming difficult to distinguish artificially manufactured material from actual videos and images.[215] Deepfakes are increasingly being used to create non-consensual sexual imagery that depict the target in a sexual way, for example, by placing women's faces on porn videos.[216]

Defamation
Defamation involves the public release and spreading of exaggerated or false information that damages a person's reputation and that has the intention of humiliating, threatening, discrediting, intimidating or punishing the survivor and in particular public figures (for example, public officials, activists and journalists).[217]

Denial of access
Leveraging the "features of a technology or platform to harm the target, usually by preventing access to essential digital tools or platforms". There are two main forms of denying access to a technological platform: (1) mass report or false reporting, consisting of the coordinated action of abusers to falsely report a target's account as abusive or otherwise harmful to try to get it suspended or shut down and (2) message bombing or flooding, consisting of "flooding" an individual or institution's phone or email accounts with unwanted messages meant to limit or block the target's ability to use that platform.[218]

Denial of Service (DoS) attacks
A cyberattack that temporarily or indefinitely causes a website or network to crash or become inoperable by overwhelming a system with data. DoS attacks can prevent people from accessing their own devices and data, and they can compromise sensitive information stored on those devices. Distributed Denial of Service (DDoS) happens when an attacker takes control of multiple users' computers in order to attack a different user's computer. This can force the hijacked computers to send large amounts of data to a particular website or send spam to targeted email addresses.[219]

Documenting or broadcasting sexual assault (rape videos)
Recording and/or disseminating images of sexual assault on social media, via text or on websites. This is an additional form of sexual violence against the victim-survivor.[220] These videos may be subsequently used to shame or extort survivors, or are sold as non-consensual porn.[221]

Doxxing or doxing
Gendered form of online harassment that consists of non-consensual disclosure of personal information involving the public release of an individual's private, personal, sensitive information, such as home and email addresses, phone numbers, employer and family member's contact information, or photos of their children and the school they attend with the purpose of locating and causing physical harm.[222]

E

Electronically enabled financial abuse
The use of the Internet and other forms of technology to exert financial pressure on a target, usually a woman involved in intimate partner abuse. This might include, for example, denying access to online accounts, manipulating credit information to create negative scores and identity theft.[223]

F

False accusations of blasphemy
Women face online threats globally, but they run a unique risk in conservative religious countries, where blasphemy is against the law and where honour killings are a serious threat. Accusing someone of blasphemy can become, itself, an act of violence.[224]

Flaming
Posting or sending offensive messages over the Internet. These messages, called "flames", may be posted within online discussion forums or newsgroups, or sent via email or instant messaging programs. The most common area where flaming takes place is online discussion forums.[225]

G

(Gendered or sexist) hate speech
Any kind of communication in speech, writing or behaviour, that attacks or uses pejorative or discriminatory language with reference to a person or a group on the basis of who they are, in this case, based on their sex, gender, sexual orientation or gender identity. Gendered and sexist online hate speech reinforces systemic sexism while dehumanizing and encouraging violence against women and girls and LGBTQIA+ people.[226]

Gender-trolling
Online abuse or harassment for "fun". Trolls deliberately post comments or message, upload images or videos and create hashtags for the purpose of annoying, provoking or inciting violence against women and girls. Trolls seem to enjoy it when people get upset about what they post, and often shrug off complaints about their behaviour, claiming it was all in fun.[227] Many trolls are anonymous and use false accounts.

Google bombing
The deliberate optimization of malicious information and websites online so that people immediately see defamatory content when they search for a target.[228]

Grooming (online)
Specific type of technology-facilitated sexual experience by which children and young people are contacted through social media or other digital platforms with the purpose of sexually assaulting them.[229] Online grooming consists of setting up an online abusive relationship with a child, in order to bring the child into sexual abuse or child-trafficking situations.[230]

H

Hacking
Use of technology to gain illegal or unauthorized access to systems or resources for the purpose of attacking, harming or incriminating another person or organization by stealing their data, acquiring personal information, altering or modifying information, violating their privacy or infecting their devices with viruses.[231]

Hashtag poisoning
The creation of an abusive hashtag, or the hijacking of an existing hashtag, which is then leveraged as a rallying cry for cybermob attacks.[232]

I

Image-based abuse (IBA)
Using images to coerce, threaten, harass, objectify or abuse a survivor. Includes a wide range of behaviours that involve taking, sharing or threatening to share intimate images without consent. These images may be sexual in nature, in which case we talk about "image-based sexual abuse".[233]

Impersonation
Process of stealing someone's identity so as to threaten or intimidate, as well as to discredit or damage a user's reputation.[234]

In-real-life (IRL) attacks
Incidents where online abuse either moves into the "real" world or is already part of an ongoing stalking or intimate partner violence interaction. IRL trolling can also mean simply trying to instil fear by letting a target know that the abuser knows their address or place of employment.[235]

L

Limiting or controlling use of technology
Perpetrators may use technology to exert abuse and control over the survivor, by tracking, monitoring or restricting the survivor's movements, communications and activities. These abusive behaviours range from forcing their partners to give their passwords and obtaining unauthorized access to their online accounts, to limiting their use of technology devices. In abusive intimate relationships, intimate privacy threats to technology use can be a precursor to other forms of abuse.[236]

M

Mobbing or dogpiling
Also called cybermobbing or networked harassment, consists of organized, coordinated and systematic attacks by a group of people against particular individuals or issues, such as by groups that target feminists or people who post about racial equality issues online.[237] Outrage or shame mobs are a form of mob justice focused on publicly exposing, humiliating and punishing a target, often for expressing opinions on politically charged topics or ideas the outrage mob disagrees with and/or has taken out of context in order to promote a particular agenda.[238]

O

Online (gender) harassment
Online gender harassment is a course of conduct that involves the use of technology to repeatedly contact, annoy, threaten or scare another person through unwelcome, offensive, degrading or insulting verbal comments and often images, and that is committed by single individuals or mobs of male perpetrators, on the basis of the target's gender, sexuality or sexual orientation.[239]

R

Recruitment
Use of technology to lure potential victims/survivors into violent situations[240] or to facilitate in-person physical or sexual assault.[241] Perpetrators and traffickers may use technology to contact potential victims through fraudulent posts and advertisements in dating sites and apps, "marriage agencies" or publish false employment and study opportunities.[242]

Retaliations against supporters of survivors
Threats or harassment towards a target's family members, friends, employers or community of supporters.[243]

S

Sexting and abusive sexting
Sexting is the consensual electronic sharing of naked or sexual photographs. This is different, however, from the non-consensual sharing of the same images. While sexting is often demonized as dangerous, the danger and infraction is actually resident in the violation of privacy and consent that accompanies the sharing of images without the subject's consent. For example, while teenage boys and girls sext at the same rates, boys are between two and three times more likely to share images that they are sent.[244]

Sextortion
It 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.[245]

Shock and grief trolling
Targeting survivors by using the names and images of lost ones to create memes, websites, fake Twitter accounts or Facebook pages.[246]

Slut-shaming online
A form of gender-based bullying often targeting teenage girls and LGBTQIA+ people, that consists of criticizing if they do not conform to social expectations regarding behaviour, appearance and sexuality, often rooted in gender norms. Slut-shaming, stalking, the use of non-consensual photography and sexual surveillance frequently overlap, amplifying impact on targets.[247]

Swatting
Placing a hoax call to law enforcement detailing a completely false threatening event taking place at a target's home or business, with the intention of sending a fully armed police unit (i.e. SWAT team) to the target's address. Harassers will report a serious threat or emergency, eliciting a law enforcement response that might include the use of weapons and possibility of being killed or hurt. Swatting is rare, but extremely dangerous, and a clear example of how online harassment has the potential to cause harm in offline life.[248]

Synthetic sexual media
Manipulation of images, making it appear as though people are engaging in sexual activity they did not engage in. Synthetic sexual media may be produced for sexual entertainment and profit, to harass women and purposely cause them harm. It can include using software to superimpose a person's face onto a sexual image. Deepfakes are a form of synthetic social media.[249]

T

Technology-facilitated unwanted sexual experiences
Use of communication technologies, such as cell phones, email, social networking sites, chat rooms or online dating sites and apps, to commit or procure sexual assault or abuse.[250]

Threats
A threat is "a statement of an intention to inflict pain, injury, damage, or other hostile action" against a target. This includes death threats, and threats of physical and/or sexual violence.[251]

U

Upskirting, creepshots and digital voyeurism
These forms of IBA and sexual surveillance involve taking non-consensual photos or videos of survivors, mainly women and girls, in public places such as stores, public bathrooms, locker rooms, classrooms or the street; but also in their own apartments. They may entail taking images up a person's dress or skirt (*upskirting*)[252], taking a sexually suggestive picture of a woman without her noticing (*creepshot*)[253] or surveilling or surreptitiously observing with the use of technological tools, and in some cases recording, another person in what would generally be regarded as a private place (*digital voyeurism*).[254]

Z

Zoom-bombing
Occurs when people join online meetings or gatherings in order to post racist, sexist, pornographic or anti-Semitic content to shock and disturb viewers, it is a form of networked harassment.[255]

Technology-related terms

A

Algorithm
An algorithm is a procedure or formula for solving a problem, that is, a series of instructions that tell a computer how to transform a data set into useful information. Algorithms are widely used throughout all areas of information technology. For example, any computer program can be viewed as an elaborate algorithm.[256]

Application or App
Software programs, generally for mobile devices, such as smartphones and tablets, where downloading and installation usually happen in the same step with no further action needed by the user and which can be removed without affecting the functioning of the device.[257]

Artificial Intelligence (AI)
Artificial intelligence is a field that combines computer science and robust data sets, to enable problem-solving. It also encompasses subfields of machine learning and deep learning, which are frequently mentioned in conjunction with artificial intelligence. Artificial intelligence seeks to create expert systems which make predictions or classifications based on input data, and leverages computers and machines to mimic the problem-solving and decision-making capabilities of the human mind.[258]

D

Digital platform
Digital platforms are online businesses that facilitate commercial interactions and exchanges of information, goods or services to occur between producers and consumers as well as the community that interacts with said platform. Digital platforms can be social media platforms (Facebook, Twitter and LinkedIn), knowledge platforms (Yahoo!Answers and Google Scholar), media sharing platforms (Spotify, YouTube and Netflix) or service-oriented platforms (Airbnb, Amazon and Uber).[259]

Digital technologies
Digital technologies are electronic tools, systems, devices and resources that generate, store or process data. They include the infrastructure, devices, media, online services and platforms that we use for communication, information, documentation, networking/relation and identity needs.[260]


1458
Options
Clear
SAMSUNG
OK

Drone

In technological terms, a drone is an unmanned aircraft – it is a flying robot that can be remotely controlled or fly autonomously through software-controlled flight plans in their embedded systems, working in conjunction with on-board sensors and GPS. Drones are more formally known as unmanned aerial vehicles (UAVs) or unmanned aircraft systems (UASs). Drones are now used in a wide range of civilian roles ranging from search and rescue, surveillance, traffic monitoring, weather monitoring and firefighting, to personal drones and business drone-based photography, as well as videography, agriculture and even delivery services.[261]

G

GPS and GPS tracking

GPS tracking is the surveillance of location through use of the Global Positioning System (GPS) to track the location of an entity or object remotely. The technology can pinpoint longitude, latitude, ground speed and course direction of the target.The GPS is a "constellation" of 24 well-spaced satellites that orbit the Earth and make it possible for people with ground receivers (or GPS tracking devices) to pinpoint their geographic location. The location accuracy is anywhere from 10 to 100 metres for most equipment. GPS equipment is now integrated in smartphones, tablets and GPS navigation devices. GPS devices in smartphones and other mobile devices are often used to track employee location, for example. Privacy advocates warn that the technology can also make it possible for advertisers, Government, hackers and cyberstalkers to track users through their mobile devices.[262]

I

Information and communication technologies

Diverse set of technological tools and resources used to transmit, store, create, share or exchange information. These technological tools and resources include computers, the Internet (websites, blogs and emails), live broadcasting technologies (radio, television and webcasting), recorded broadcasting technologies (podcasting, audio and video players and storage devices) and telephony (e.g. fixed or mobile, satellite and visio/video-conferencing).[263]

O

Online platform

An online platform is a digital service that facilitates interactions between two or more distinct but interdependent sets of users (whether firms or individuals) who interact through the service via the Internet. The term "online platform" has been used to describe a range of services available on the Internet, including marketplaces, search engines, social media, creative content outlets, app stores, communications services, payment systems, services comprising the so-called "collaborative" or "gig" economy, and much more.[264]

P

Private technology companies, or tech companies[265]

Private technology companies encapsulate a wide range of organizations including, but not limited to the following:

- designated Internet service providers: entities who allow end users to access online materials, and Internet service providers, being those entities who supply Internet carriage services including among others, Google, Safari and Internet Explorer;
- social media service providers: entities who provide services that connect two end users through online means including among others, Facebook, LinkedIn and Instagram;
- electronic service providers: entities who allow end users to communicate with one another (e.g. Outlook and gaming chat services);
- app distribution service providers: entities who provide access to app services including among others, Google (through the Google PlayStore) and Apple (through IOS App Store);
- hosting service providers: entities who enable hosting of stored materials provided on social media services, relevant electronic services or designated Internet services including, among others, Apple and Microsoft each through their provision of cloud services;
- hardware development companies: entities who create, develop and/or maintain technology equipment, physical assets and other tangible items;
- software development companies: entities who create, design, develop and maintain programmes, applications, frameworks or other software components.

S

Social media

Social media is a collective term for websites and applications that focus on Internet-based communication, community-based input, interaction, content-sharing and collaboration. Forums, microblogging, social networking, social bookmarking, social curation and wikis are among the different types of social media that allow quick electronic communication of content to users. Content includes personal information, documents, videos and photos. Users engage with social media via a computer, tablet or smartphone via web-based software or applications. The most commonly used social media platforms are Facebook, YouTube, WhatsApp, Facebook Messenger, Instagram and TikTok.[266]

Spyware

Spyware is a type of malicious software that is installed on a computing device without the end user's knowledge. It invades the device, steals sensitive information and Internet usage data, and relays it to advertisers, data firms or external users. Once installed, it monitors Internet activity, tracks login credentials and spies on sensitive information.

Spyware can also be used to track a person's location, as is the case with **stalkerware**. Stalkerware is often installed secretly on mobile phones by spouses, intimate partners, ex-partners and even parents or family members. This type of spyware can track the physical location of the survivor, intercept their emails and texts, eavesdrop on their phone calls and record conversations, and access personal data, such as photos and videos.[267]

195 OHCHR (2018). Report of the Special Rapporteur on violence against women (see footnote 11).

196 Flynn, Powell and Hindes, Technology-facilitated abuse (see footnote 3).

197 United Nations Human Rights Council. Report by Special Rapporteur Dubravka Šimonović (18 June 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. UN Doc A/HRC/38/47.

198 https://eige.europa.eu/publications/cyber-violence-against-women-and-girls

199 L. Hinson, J. Mueller, L. O'Brien-Milne and N. Wandera (2018). Technology-facilitated Gender-based Violence: What Is It, and How Do We Measure it? (Washington D.C.: International Center for Research on Women). Available at: https://www.svri.org/sites/default/files/attachments/2018-07-24/ICRW_TFGBVMarketing_Brief_v8-Web.pdf

200 https://violenciadigital.tedic.org/indexEng.html#violencia

201 Anastasia Powell, Adrian J. Scott and Nicola Henry, "Digital harassment and abuse: experiences of sexuality and gender minority adults", European Journal of Criminology, vol. 17, No. 2, (2018), pp. 199–223. https://journals.sagepub.com/doi/full/10.1177/1477370818788006

202 Association for Progressive Communications (2017). Online gender-based violence: A submission from the Association for Progressive Communications to the United Nations Special Rapporteur on violence against women, its causes and consequences. Available at: https://www.apc.org/sites/default/files/APCSubmission_UNSR_VAW_GBV_0_0.pdf

203 J. Bailey, A. Flynn and N. Henry, "Prelims", in The Emerald International Handbook of Technology Facilitated Violence and Abuse, J. Bailey, A. Flynn and N. Henry, eds. (Bingley, Emerald Publishing Limited, 2021) pp. i–xxiv. https://doi.org/10.1108/978-1-83982-848-520211059

204 Penn America. Online Harassment Field Manual. Available at: https://onlineharassmentfieldmanual.pen.org/defining-online-harassment-a-glossary-of-terms/

205 eSafety Commission Australia. Catfishing. Available at: https://www.esafety.gov.au/young-people/catfishing

206 Penn America, Online harassment field manual.

207 Cyberbullying Research Centre. What is cyberbullying? Available at: https://cyberbullying.org/what-is-cyberbullying

208 Van der Wilk, Cyber violence and hate speech online against women (see footnote 52).

209 Penn America, Online harassment field manual.

210 Flynn, Powell and Hindes, Technology-facilitated abuse (see footnote 3).

211 Women's Media Centre. WMC Speech Project: Online Abuse 101. Available at: https://womensmediacenter.com/speech-project/online-abuse-101

212 VAW Learning Network, Technology-related violence against women (see footnote 20) Henry and Powell, Technology-facilitated sexual violence (see footnote 22).

213 Ibid.

214 Women's Media Centre, WMC Speech Project.

215 John R. Allen and Darrell M. West (2020). The Brookings glossary of AI and emerging technologies. Available at: https://www.brookings.edu/blog/techtank/2020/07/13/the-brookings-glossary-of-ai-and-emerging-technologies/

216 Flynn, Powell and Hindes, Technology-facilitated abuse (see footnote 3).

217 Douglas, Doxing: a conceptual analysis (see footnote 40). Dunn, Technology-facilitated gender-based violence: an overview (see footnote 24).

218 Penn America, Online harassment field manual.

219 Ibid.

220 GBV AoR Helpdesk, Learning Series on Technology-Facilitated Gender-Based Violence (see footnote 100).

221 Women's Media Centre, WMC Speech Project.

222 MacAllister, The doxing dilemma (see footnote 38).

Douglas, Doxing: a conceptual analysis (see footnote 40).

223 Women's Media Centre, WMC Speech Project.

224 Ibid.

225 https://techterms.com/definition/flaming

226 UN, United Nations Strategy and Plan of Action on Hate Speech (see footnote 58).

227 eSafety Commission Australia. Online abuse targeting women. Available at: https://www.esafety.gov.au/women/online-abuse-targeting-women

228 Women's Media Centre, WMC Speech Project.

229 Craven, Brown and Gilchrist, Sexual grooming of children (see footnote 36).

230 Van der Wilk, Cyber violence and hate speech online against women (see footnote 52).

231 Penn America, Online harassment field manual.

VAW Learning Network, Technology-related violence against women (see footnote 20).

232 Penn America, Online harassment field manual.

233 Flynn, Powell, and Hindes, Technology-facilitated abuse (see footnote 3).

McGlynn, Rackley, and Houghton, Beyond revenge porn (see footnote 9).

234 Van der Wilk, Cyber violence and hate speech online against women (see footnote 52).

235 Women's Media Centre, WMC Speech Project.

236 Levy and Schneier, Privacy threats in intimate relationships (see footnote 62).

237 GBV AoR Helpdesk, Learning Series on Technology-Facilitated Gender-Based Violence (see footnote 100).

238 Penn America, Online harassment field manual.

239 VAW Learning Network, Technology-related violence against women (see footnote 20). Henry and Powell, Technology-facilitated sexual violence (see footnote 22). Flynn, Powell and Hindes, Technology-facilitated abuse (see footnote 3).

240 VAW Learning Network, Technology-related violence against women (see footnote 20).

241 Fascendini and Fialová, Voices from digital spaces (see footnote 14).

242 APC, How technology is being used to perpetrate violence against women (see footnote 48).

243 Women's Media Centre, WMC Speech Project.

244 Ibid.

245 Dunn, Technology-facilitated gender-based violence: an overview (see footnote 24).

246 Women's Media Centre, WMC Speech Project.

247 Ibid.

248 Women's Media Centre, WMC Speech Project.Penn America, Online harassment field manual.

249 Dunn, Technology-facilitated gender-based violence: an overview (see footnote 24).

250 Henry, Flynn, and Powell, Technology-facilitated domestic and sexual violence (see footnote 32).

251 Penn America, Online harassment field manual.

252 Flynn, Powell and Hindes, Technology-facilitated abuse (see footnote 3).

253 Lexico. https://www.lexico.com/definition/creepshot

254 Clough,J (2015). Harassment, In Principles of Cybercrime (pp. 417 – 453). Cambridge: Cambridge University Press. doi:10.1017/CBO9781139540803.013.

255 Dunn, Technology-facilitated gender-based violence: an overview (see footnote 24).

256 The Conversation (2020). What is an algorithm? How computers know what to do with data. Available at: https://theconversation.com/what-is-an-algorithm-how-computers-know-what-to-do-with-data-146665

257 Techopedia (2012). App. Available at: https://www.techopedia.com/definition/28104/app

258 IBM (2020). Artificial Intelligence (AI). Available at: https://www.ibm.com/cloud/learn/what-is-artificial-intelligence

259 BMC blogs (2020). Digital Platforms: A Brief Introduction. Available at: https://www.bmc.com/blogs/digital-platforms/#

260 GBV AoR Helpdesk, Learning Series on Technology-Facilitated Gender-Based Violence (see footnote 100).

261 IoT Agenda (2019). Drone (UAV). Available at: https://internetofthingsagenda.techtarget.com/definition/drone

262 WhatIs.com (2014). GPS tracking. Available at: https://whatis.techtarget.com/definition/GPS-tracking

263 UNESCO Institute for Statistics. Glossary: Information and communication technologies (ICT). Available at: http://uis.unesco.org/en/glossary

264 OECD (2019). An Introduction to Online Platforms and Their Role in the Digital Transformation. Available at: https://www.oecd-ilibrary.org/science-and-technology/an-introduction-to-online-platforms-and-their-role-in-the-digital-transformation_53e5f593-en

265 Online Safety Act 2021 (Cth). No. 76, 2021. (Austl.)

266 GBV AoR Helpdesk, Learning Series on Technology-Facilitated Gender-Based Violence (see footnote 108).

267 TechTarget (2021). Spyware. Available at: https://searchsecurity.techtarget.com/definition/spyware

United Nations Population Fund
605 Third Avenue, New York, NY 10158
1-212-297-5000 / www.unfpa.org / @UNFPA