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

Association for Progressive Communications (APC)
November 2017

Table of contents

1. Background to the submission

The Association for Progressive Communications' Women's Rights Programme (APC WRP) has worked to render visible the impact of online gender-based violence (GBV) on women's rights for more than a decade. We have worked with women's organisations and advocates to identify, monitor, analyse and combat uses of the internet and digital technologies that are harmful to women and marginalised communities, and with individual internet users to assist them in using technology to document and combat online GBV and challenge harmful sexist online practices. We have also advocated for internet policy and regulation that enable the expression, protection and promotion of human rights, women's rights, and the rights of people of diverse sexualities to both states and private sector actors. Over the past few years particularly, we have seen how online GBV has moved from a peripheral discussion in both the women's rights and internet rights communities to occupying a central space in conversations about a free and open internet.

This submission[1] draws on the above experience as well as that of working with partners in the global South to understand, respond to and prevent online GBV. It takes the perspective that online GBV is part of the continuum of violence against women and as such occurs in all countries, contexts and settings, is one of the most pervasive violations of human rights, and is a "manifestation of the historically unequal power relations between men and women and systemic gender-based discrimination."[2]

There are multiple terms used to describe the kinds of abuse and harassment experienced by women and girls online. These include cyber violence, online violence, technology-related violence, technology-mediated violence against women, e-VAW and others. We employ the following definition[3] of technology-related violence against women[4] as encompassing:

> Acts of gender-based violence that are committed, abetted or aggravated, in part or fully, by the use of information and communication technologies (ICTs), such as mobile phones, the internet, social media platforms, and email.

[1]This submission was prepared with support from the Swedish International Development Cooperation Agency (Sida).

[2]Prevention of violence against women and girls: Report of the Secretary-General. Commission on the Status of Women, Fifty-seventh session, 4-15 March 2013. undocs.org/E/CN.6/2013/4

[3]Association for Progressive Communications. (2015). *From impunity to justice: Exploring corporate and legal remedies for technology-related violence against women*. https://www.genderit.org/onlinevaw

[4]While APC initially used the term "technology-related violence against women" (see https://www.genderit.org/onlinevaw), more recently we refer to "online gender-based violence" to communicate our intersectional understanding of violence against women which considers race, class, sexuality, age and other locations, to be able to reflect the findings of research on sexual rights and the internet (see erotics.apc.org) and also, because the term "online" has become more commonly understood and used. It must be noted, however, that we deliberately chose to use "technology-related" versus "online" or "on the internet" until 2015 in order to a) recognise that this violence can affect women who are not "online" themselves; b) incorporate those experiences that were impacted by digital technologies that did not make use of the internet, such as digital recordings, sharing via Bluetooth or other means, etc. (see for example the case study from Pakistan, "When a sex video is used as blackmail", available at https://www.genderit.org/sites/default/upload/case_studies_pak3_1.pdf); and c) avoid falling into a binary of online vs. offline violence that can feed the perception that these expressions of violence are distinct and separate from systemic gender-based discrimination. Although we use the term "online" currently, it incorporates these considerations as well. We argue that more work needs to be done to describe this type of violence in order to reflect this multiplicity of experience.

2. Context

Since APC's work on this issue began more than 10 years ago, one of the most significant shifts has been from viewing women's experiences of violence online as a series of isolated incidents affecting relatively privileged women, to an understanding that these are part of the wider context of unequal power relations and systemic gender-based violence and discrimination.

There is growing acceptance that the same forms of gender discrimination in social, economic, cultural and political structures that result in gender-based violence are reproduced, and sometimes amplified, online. Women and girls face specific threats including online harassment, cyberstalking, attacks on their sexuality, exposure of personal information, threats based on morality or religion, manipulation of images, non-consensual distribution of intimate images or distribution "sex videos" that are used for blackmail and can result in repeated trauma every time they are reposted online.[5] While the gender-based violence is not new, the technology dimension adds elements of searchability, persistence, replicability and scalability[6] which facilitate aggressors' access to women they are targeting and can escalate and exacerbate harm.

LBTs, sex workers and others who use the internet to access information, socialise, build communities and advance the rights of marginalised women experience particular risk. Their critical work on issues that are often deeply taboo/contested in their contexts, and lack of access to other kinds of public spaces for the exchange of information and organising, makes it essential to respond to the specific risks they face online.[7] In the digital age, the normalisation of violent behaviour and the culture that tolerates violence against women that social media perpetuates and facilitates at rapid speed, work to reinforce sexist and violent attitudes, and contribute to norms and practices that make online and offline spaces hostile towards women and communities most at risk of injustice and discrimination.

2.1. What constitutes online gender-based violence?

A report from the Internet Governance Forum (IGF) Best Practice Forum on online abuse and gender-based violence lists a number of actions that form part of online gender-based violence.[8] Significantly, the report notes, "these acts are often an extension of existing gender-based violence, such as domestic violence, stalking and sexual harassment, or target the victim on the basis of her gender or sexuality." The report lists the following acts:

Infringement of privacy:

- Accessing, using, manipulating and/or disseminating private data without consent (by cracking[9] personal accounts, stealing passwords, using/stealing identities, using another person's computer to access a user's accounts while it is logged in, etc.)

[5]See Fascendini, F., & Fialova, K. (2013). *Voices from digital spaces: Technology-related violence against women*. Association for Progressive Communications. https://www.genderit.org/resources/voices-digital-spaces-technology-related-violence-against-women

[6]boyd, d. (2010). *Social Network Sites as Networked Publics.* https://www.danah.org/papers/2010/SNSasNetworkedPublics.pdf

[7]See Kee, J. (ed.). (2011). *EROTICS: Sex, rights and the internet – An exploratory research study*. Association for Progressive Communications. erotics.apc.org/research/erotics

[8]Internet Governance Forum (IGF) 2015: Best Practice Forum (BPF) on Online Abuse and Gender-Based Violence Against Women. https://www.intgovforum.org/cms/documents/best-practice-forums/623-bpf-online-abuse-and-gbv-against-women/file

[9]The term "cracking" is used rather than "hacking" to indicate a forced entry or takeover of content with malicious intent, while "hacking" could include similar actions that are bona fide and/or done in the public interest.

- Taking, accessing, using, manipulating, and/or disseminating photographs and/or videos without consent (including "revenge pornography")
- Sharing and/or disseminating private information and/or content, including (sexualised) images, audio clips and/or video clips, without knowledge or consent
- Doxing (researching and broadcasting personally identifiable information about an individual without consent, sometimes with the intention of providing access to the woman in the "real" world for harassment and/or other purposes)
- Contacting and/or harassing a user's children, extended family, colleagues (etc.) to gain access to her.

Surveillance and monitoring:

- Monitoring, tracking and/or surveillance of online and offline activities
- Using spyware or keyboard loggers without a user's consent
- Using GPS or other geolocator software to track a woman's movements without consent
- Stalking.

Damaging reputation and/or credibility:

- Deleting, sending and/or manipulating emails and/or content without consent
- Creating and sharing false personal data (like online accounts, advertisements, or social media accounts) with the intention of damaging a user's reputation
- Manipulating and/or creating fake photographs and/or videos
- Identity theft (e.g. pretending to be the person who created an image and posting or sharing it publicly)
- Disseminating private (and/or culturally sensitive/controversial) information for the purpose of damaging someone's reputation
- Making offensive, disparaging and/or false online comments and/or postings that are intended to tarnish a person's reputation (including libel/defamation).

Harassment (which may be accompanied by offline harassment):

- "Cyber bullying" and/or repeated harassment through unwanted messages, attention and/or contact
- Direct threats of violence, including threats of sexual and/or physical violence (e.g. threats like "I am going to rape you")
- Abusive comments
- Unsolicited sending and/or receiving of sexually explicit materials
- Incitement to physical violence
- Hate speech, social media posts and/or mail; often targeted at gender and/or sexuality
- Online content that portrays women as sexual objects
- Use of sexist and/or gendered comments or name-calling (e.g. use of terms like "bitch"/"slut")
- Use of indecent or violent images to demean women
- Abusing and/or shaming a woman for expressing views that are not normative, for disagreeing with people (often men) and also for refusing sexual advances

- Counselling suicide or advocating femicide
- Mobbing, including the selection of a target for bullying or harassment
- Mobbing by a group of people rather than an individual and as a practice specifically facilitated by technology.

Direct threats and/or violence:

- Trafficking of women through the use of technology, including use of technology for victim selection and preparation (planned sexual assault and/or femicide)
- Sexualised blackmail and/or extortion
- Theft of identity, money and/or property
- Impersonation resulting in physical attack.

Targeted attacks to communities:

- Cracking[10] websites, social media and/or email accounts of organisations and communities with malicious intent
- Surveillance and monitoring of activities by members of the community
- Direct threats of violence to community members
- Mobbing, specifically when selecting a target for bullying or harassment by a group of people, rather than an individual, and as a practice specifically facilitated by technology
- Disclosure of anonymised information like addresses of shelters, etc.

2.2. Harm

A key finding of APC's research on online GBV is that it infringes on women's right to self-determination and bodily integrity, impacts on their capacity to move freely, without fear of surveillance, and denies them the opportunity to craft their own identities online, and to form and engage in socially and politically meaningful interactions.[11] Recent legislative trends also show recognition that harm caused by harassment online includes emotional distress, even if there is no physical harm.[12] Moreover, women do not even have to be internet users to suffer online violence (e.g. the distribution of rape videos online unbeknownst to the victims/survivors).

Based on analysis of 1,126 cases reported via the Take Back the Tech online mapping platform and 24 in-depth case studies,[13] we have identified some types of harm experienced as a result of online GBV. These include, among others:[14]

- *Psychological harm* through which victims/survivors experience depression, anxiety and fear. There was also a certain point where some victims/survivors expressed suicidal thoughts as a result of the harm they faced. One woman recounts, "I considered committing suicide, because I figured that this would send the message that this wasn't a game."[15]

[10]Ibid.

[11]Maholtra, N. (2015). *Good questions on technology-related violence*. Association for Progressive Communications. https://www.genderit.org/sites/default/upload/end_violence_malhotra_dig.pdf

[12]Nyst, C. (2015). *Technology-related violence against women: Recent legislative trends*. Association for Progressive Communications. https://www.genderit.org/sites/default/upload/flowresearch_cnyst_legtrend_ln.pdf

[13]See https://www.genderit.org/onlinevaw/countries

[14]Note that the research (and APC's area of focus) does not focus on/include trafficking or grooming.

- *Social isolation* through which victims/survivors withdrew from public life, including with family and friends. This was particularly true for women whose photos and videos were distributed without their consent who felt publicly humiliated and ridiculed. As shared in a case study: "I felt like I lost something, perhaps my confidence. For one year, I did not talk to people. I felt there was nothing for me to say so I did not talk."[16]
- *Economic loss* through which victims/survivors became unemployed and lost income. For example, Ruby* was forced to resign from her job after sex videos were distributed online without her consent. She said: "I had been working for [only] five years and I did not expect to lose my job. All my contracts ended at the same time, just when the scandal erupted."[17]
- *Limited mobility* through which victims/survivors lost the ability to move around freely and participate in online and/or offline spaces. In one case, the survivor's education came to an end because her father believed it was her freedom to commute to school that had ultimately led to the violence – and by extension, the "shame" suffered by the family.[18]
- *Self-censorship* for fear of further victimisation and due to loss of trust in the safety of using digital technologies, which was the case of Alejandra, who completely withdrew from the internet for a long period of time.[19] Removing oneself from the internet has further implications beyond self-censorship, such as access to information, e-services, and social or professional communication.

In addition to the impact on individuals, a major consequence of online gender-based violence is the creation of a society where women no longer feel safe online and/or offline. According to the Internet Governance Forum Best Practice Forum on online abuse:

> It also contributes towards a culture of sexism and misogyny online and, in offline spaces, to existing gender inequality. In respect of the latter, online abuse and gender-based violence disadvantage women in limiting their ability to benefit from the same opportunities online that men frequently benefit from (e.g. employment, self-promotion and/or self-expression).[20]

2.3. Who is affected?

APC's research[21] highlights three types of people who are most at risk of experiencing online gender-based violence. The following table provides a summary.

[15]Si Jeunesse Savait. (2014). Case study number 1, DRC. Unpublished; case study summary available at: https://www.genderit.org/node/4253

[16]Foundation for Media Alternatives. (2014). Case study number 2, the Philippines. Unpublished; case study summary available at: https://www.genderit.org/node/4240

[17]Ibid.

[18]Bukhari, G. (2014). Case study number 3, Pakistan. Unpublished; case study summary available at: https://www.genderit.org/node/4239

[19]Colnodo. (2014). Case study number 3, Colombia. Unpublished; case study summary available at: https://www.genderit.org/sites/default/upload/case_studies_col3_1.pdf

[20]https://www.intgovforum.org/cms/documents/best-practice-forums/623-bpf-online-abuse-and-gbv-against-women/file

[21]See https://www.genderit.org/sites/default/upload/csw_map.pdf

Identity of person	What is at stake	What happens	Consequences
Someone involved in an intimate relationship	Intimacy and trust	Involves use of ICTs for private expression, the content of which is then exploited publicly by someone who was intimately involved with that person.	Can result in extreme consequences (e.g. suicide), and widespread sense of public shame. May require severe action such as changing name and address.
Professional, often involved in public expression; includes activists, journalists, writers, researchers, musicians, actors, or anyone with a public profile or interest in public exchange	Freedom of expression: personal and political	Harassment, threats, silencing through verbal abuse.	Typically appears to result in less extreme consequences for the victims given their public status, a greater sense of empowerment to remedy the situation.
Survivor/victim of physical assault	Physical safety	Involves direct crime, such as filming a gang rape.	Can result in extreme consequences, such as suicide of the person violated.

Since this research was conducted, however, there is evidence to suggest that those involved in public expression can experience similar consequences to the others, given that the degree and nature of the threats and harassment are similar.

A 2016 Inter-Parliamentary Union survey[22] found that social media has become the primary space in which psychological violence – including sexist and misogynistic remarks, humiliating images, mobbing, threats and intimidation – is perpetrated against women parliamentarians. A European MP shared, "One time, over a period of four days, I received more than 500 threats of rape on Twitter," while a parliamentarian from Asia said, "I receive information about my son – his age, the school he attends, his class, etc. – threatening to kidnap him."

According to the survey:

- 41.8% report wide distribution of "extremely humiliating or sexually charged images"
- 44.4% receive death, rape, beating and abduction threats
- 32.7% have been harassed through exposure to persistent unwanted and intimidating messages
- 61.5% believe that the primary objective of the harassment they face is to dissuade women from pursuing political leadership positions.

Similarly, a global survey on harassment and violence against female media workers conducted by the International Women's Media Foundation[23] showed that more than 25% of "verbal, written and/or physical intimidation including threats, to family or friends" took place online. More than one in five respondents said they had experienced digital/online account surveillance.

For activists working on gender, sexuality and sexual rights who use the internet in their work, the situation is also similar. A global survey on sexual rights and the internet undertaken by APC in 2017

[22]Inter-Parliamentary Union. (2016). *Sexism, harassment and violence against women parliamentarians*. https://www.ipu.org/resources/publications/reports/2016-10/sexism-harassment-and-violence-against-women-parliamentarians

[23]International Women's Media Foundation. (2013). *Violence and Harassment against Women in the News Media: A Global Picture*. https://www.iwmf.org/blog/2014/03/07/intimidation-threats-and-abuse

revealed that 75% of the respondents mentioned online harassment and 63% intimidating comments when asked about the violent situations they experience.[24] This is an increase from the 51% of respondents who said they had received violent messages, threats or offensive comments while working online in the first survey in 2013.[25]

An Egyptian activist who participated in this survey shared her experience:

> When I started to talk about bodily rights in 2012 I started to be targeted personally, my account suffered hacking attempts. Every discussion I make on the internet has cyber bullying against me (…). When I broke with my boyfriend, he was mad with me because he wanted me to be in the religion with him. When I refused he started to threaten me with some private content: nude photos and a video showing me dancing.

The victims/survivors of online GBV cut across race, gender expression, age, location, ability, sexual orientation and other locations. At the same time, discrimination based on any of these locations also exacerbates experiences of online GBV. It is therefore essential that any responses, both legal and non-legal, take into consideration how multiple and intersecting forms of discrimination can intensify experiences of online gender-based violence.

2.4. State responses[26]

The state has an obligation to promote, protect and fulfil human rights. This includes the obligation to prevent violations, protect victims/survivors of human rights abuses, prosecute violations, punish perpetrators and provide redress and reparation for victims/survivors.[27] This also includes the obligation to remove impunity and provide for certainty of punishment of perpetrators of violence against women.

The due diligence principle obligates states to take reasonable measures to prevent violence before it occurs, such as adopting relevant laws and policies, and effectively prosecuting and punishing perpetrators once it occurs as well as providing redress and reparation to victims/survivors. Failure to exercise due diligence in taking these measures would render a state accountable.

But despite this, from reporting to prosecution, overall the findings of the seven-country APC research[28] which explored the extent to which victims/survivors were able to access justice in relation to online GBV show a grossly inadequate response by states. The following findings, while based on the seven

---

[24]Schenone Sienra, D., & Palumbo, M. (2017). *EROTICS Global Survey 2017: Sexuality, rights and internet regulations*. Association for Progressive Communications. https://www.apc.org/en/pubs/erotics-global-survey-2017-sexuality-rights-and-internet-regulations

[25]Association for Progressive Communications. (2013). Survey on sexual activism, morality, and the internet. https://www.genderit.org/articles/survey-sexual-activism-morality-and-internet

[26]This section is based on the findings of the APC seven-country study into online violence against women, specifically the report on domestic legal remedies available here https://www.genderit.org/onlinevaw/state; Abdul Aziz, Z. (2016). *Due diligence and accountability for online violence against women*. Association for Progressive Communications. https://www.apc.org/sites/default/files/DueDiligenceAndAccountabilityForOnlineVAW.pdf; and Internet Governance Forum (IGF) 2015: Best Practice Forum (BPF) on Online Abuse and Gender-Based Violence Against Women. www.intgovforum.org/cms/documents/best-practice-forums/623-bpf-online-abuse-and-gbv-against-women/file

[27]Abdul Aziz, Z., & Moussa, J. (2013). *Due Diligence Framework: State Accountability Framework for Eliminating Violence against Women*. International Human Rights Initiative. https://duediligenceproject.org/ewExternalFiles/Due%20Diligence%20Framework%20Report%20Z.pdf

[28]The research took place in the Democratic Republic of Congo, Kenya, the Philippines, Pakistan, Colombia, Mexico and Bosnia and Herzegovina. For more information see: https://www.genderit.org/onlinevaw

countries, can be extrapolated to reflect the experiences of the majority of victims/survivors in the global South. This is reflected also in anecdotal evidence.

Despite the existence of laws that can be applied in cases of technology-related VAW, the incompetence of duty bearers presents a significant barrier to women's access to justice. Law enforcement typically trivialises technology-related VAW and victim blaming is common among police personnel. This attitude results in a culture of silence, where survivors are inhibited from speaking out for fear of being blamed for the violence they have experienced.

Moreover, authorities fail to make use of available laws, either due to indifference or a lack of awareness around the existence of relevant legislation. In particular, cybercrime units deal only with technical or commercially motivated crimes, and do not specialise in technology-related VAW.

Law enforcement officers often discriminate against poor and marginalised women, and are less likely to record their cases without support from influential community members. Moreover, in the case of poorer women, the costs of litigation and the distance of available legal services prevent victims/survivors from pursuing cases.

When victims do manage to have an incident reported and investigated by law enforcement officials, they face further difficulties in terms of the abilities and technological knowledge of mediators and/or the judiciary (including court systems, magistrates, judges and other officers of law). For example, some judges faced with deciding a case about defamatory and abusive posts on a Facebook wall might struggle to understand the potential impact of such a form of abuse, and similarly, in making rulings and issuing judgements, tend to neglect the realities of how online posts are distributed on the internet. The pace at which many cases can be investigated and heard, and the costs of judicial proceedings, are furthermore prohibitive for many victims.

Existing laws that address the violation of related rights (such as laws related to privacy, misuse of network systems and services, copyright and "obscenity") and that are sometimes recommended for use to address online abuse and gender-based violence, neglect the gender-specificity of these acts, and fail to provide adequate redress for the harms that are faced. For example, obscenity laws that are used to criminalise sexual content often do not distinguish between consent and lack of consent in the creation and distribution of content. This can have the effect of criminalising consensual sexual expression of women, and can render both the victim and perpetrator as equally liable for the violation. Laws addressing cybercrime and the revelation of confidential information will only consider state or company secrets as violations, not that of individuals. In another example, women are sometimes forced to use problematic copyright laws to remove sexualised images of themselves that were published online without their consent.

In addition to the cost and jurisdictional challenges of accessing these laws, victims/survivors are also compelled to send the same images to relevant authorities to establish copyright ownership, potentially extending the impact of the harm. Facebook is currently piloting a protocol to reduce dissemination of non-consensual intimate images in Australia, which entails women uploading their own nude photos, in and of itself a security risk, thus giving Facebook personnel access to the images, in order to ensure they are never circulated on the platform.[29]

[29]For more on Facebook's policy on non-consensual dissemination of intimate images, see: https://motherboard.vice.com/en_us/article/7x478b/facebook-revenge-porn-nudesref

3. Tracing the development of a global normative framework on online gender-based violence

In 2006, the UN Secretary-General's in-depth study on violence against women[30] noted:

> More inquiry is needed about the use of technology, such as computers and cell phones, in developing and expanding forms of violence. Evolving and emerging forms of violence need to be named so that they can be recognised and better addressed.

For the next six years, until 2012, two key issues in relation to women and technology gained traction: the role of technology in the sexual exploitation of women and girls for the purposes of trafficking, sex tourism and child pornography;[31] and women and girls' equal participation in, access to and use of information and communication technologies.[32]

Since then, the recognition that online GBV is a barrier to women and LGBTIQ people's ability to benefit from the enabling potential of digital technologies has grown exponentially.

A significant moment in this shift was the 2011 report to the UN Human Rights Council (HRC) by the Special Rapporteur on the promotion and protection of the right to freedom of expression and opinion, Frank La Rue, which described the internet as "acting as a catalyst for individuals to exercise their right to freedom of opinion and expression" and through this "facilitating the realisation of a range of other human rights."[33] This was followed by the 2012 HRC resolution on the promotion, protection and enjoyment of human rights on the internet,[34] which affirmed that the same rights people have offline must also be protected online. The resolution also recognised "the global and open nature of the internet as a driving force in accelerating progress towards development in its various forms."

This understanding of the internet and digital technologies as enablers of rights, and the digital space as an extension of rights held offline, opened the door for the elaboration of how digital technologies were impacting on women's rights,[35] specifically in relation to gender-based violence.

In 2013, the Working Group on the issue of discrimination against women in law and practice's thematic report[36] to the Human Rights Council referred to the internet as having become "a site of diverse forms of violence against women, in the form of pornography, sexist games and breaches of privacy." The report highlighted the risk of harassment faced by women who engage in public debate through the internet and, significantly, the safety that anonymity provides for those who face discrimination due to their sexual orientation, as it allows them to "freely speak out, establish virtual communities and participate in public debates."

---

[30]United Nations General Assembly (UNGA). (2006). In-depth study of all forms of violence against women (A/61/122/Add.1). www.un.org/womenwatch/daw/vaw/SGstudyvaw.htm

[31]For example, A/HRC/RES/11/3 and A/HRC/RES/14/2.

[32]For example, A/HRC/RES/23/2 and A/RES/65/141.

[33]A/HRC/17/27, available at: https://www.un.org/ga/search/view_doc.asp?symbol=A/HRC/17/27

[34]A/HRC/RES/20/8, available at: undocs.org/en/A/HRC/RES/20/8

[35]See the 2013 edition of Global Information Society Watch (GISWatch), published by the Association for Progressive Communications and the Humanist Institute for Development Cooperation (Hivos), which focused on women's rights, gender and technology, available at: https://giswatch.org/2013-womens-rights-gender-and-icts

[36]A/HRC/23/50, available at: www.ohchr.org/Documents/Issues/Women/WG/A.HRC.23.50_English.pdf

In the same year, the 57th session of the Commission on the Status of Women[37] called on governments to use information and communication technologies, including social media, to empower women and to:

> [D]evelop mechanisms to combat the use of information and communications technology and social media to perpetrate violence against women and girls, including the criminal misuse of information and communications technology for sexual harassment, sexual exploitation, child pornography and trafficking in women and girls, and emerging forms of violence, such as cyberstalking, cyberbullying and privacy violations that compromise the safety of women and girls.

The UN General Assembly's December 2013 resolution on protecting women human rights defenders[38] went further to state:

> [I]nformation-technology-related violations, abuses, discrimination and violence against women, including women human rights defenders, such as online harassment, cyberstalking, violation of privacy, censorship and the hacking of e-mail accounts, mobile phones and other electronic devices, with a view to discrediting them and/or inciting other violations and abuses against them, are a growing concern and can be a manifestation of systemic gender-based discrimination, requiring effective responses compliant with human rights.

Already in 2013, states were urged to promote, respect and ensure the exercise of women's right to freedom of opinion and expression online through the HRC resolution on the role of freedom of opinion and expression in women's empowerment.[39] Given the concerns that some freedom of expression advocates have about particular responses to online GBV, which can act to censor and shut down speech, this resolution is significant as it sets the foundation for developing responses to the chilling effect that online GBV has on women's speech.

In 2015, the HRC resolution on accelerating efforts to eliminate all forms of violence against women[40] recognised that domestic violence can include acts such as cyberbulling and cyberstalking. This resolution was particularly significant as its articulation of cyberstalking as being part of a pattern of domestic violence explicitly reinforces the framing of online GBV as being part of the continuum of violence against women, and as such is already part of state responsibility to prevent and address this violence.

A year later, in 2016, the UN General Assembly's resolution on the right to privacy in the digital age[41] recognised that while all individuals may experience violations and abuses of the right to privacy, women, children and others who are vulnerable and marginalised are particularly affected by such violations and

---

[37] E/2013/27-E/CN.6/2013/11, available at https://www.un.org/womenwatch/daw/csw/csw57/CSW57_Agreed_Conclusions_%28CSW_report_excerpt%29.pdf

[38] See Promotion of the Declaration on the Right and Responsibility of Individuals, Groups and Organs of Society to Promote and Protect Universally Recognized Human Rights and Fundamental Freedoms: Protecting women human rights defenders, available at: www.un.org/en/ga/search/view_doc.asp?symbol=A/RES/68/181

[39] A/HRC/RES/23/2, available at: https://documents-dds-ny.un.org/doc/UNDOC/GEN/G13/150/77/PDF/G1315077.pdf?OpenElement

[40] A/HRC/RES/29/14, available at: https://documents-dds-ny.un.org/doc/UNDOC/LTD/G15/140/16/PDF/G1514016.pdf?OpenElement

[41] A/C.3/71/L.39/Rev.1, available at: www.un.org/ga/search/view_doc.asp?symbol=A/C.3/71/L.39/Rev.1

abuses. It calls on all states to further develop or maintain preventive measures and remedies for such violations and abuses. It is encouraging that the resolution recognises the gender dimension of this issue.

The HRC reaffirmed this language with its own resolution on the same topic in March 2017.[42] Threats to privacy and the disclosure of personal information, such as the malicious and non-consensual distribution of private sexual content through ICTs, can particularly subject women of diverse sexualities and gender identities to significant threats, including violence, harassment, intimidation and silencing both in the offline and online contexts.

In June 2017, the report of the United Nations High Commissioner for Human Rights on ways to bridge the gender digital divide from a human rights perspective[43] highlighted that online violence against women must be dealt with in the broader context of offline gender discrimination and violence, and that states should enact adequate legislative measures and ensure appropriate responses to address the phenomenon of violence against women online, including through investigation of and action against perpetrators, the provision of redress and reparations to victims, and training on the application of international human rights norms and standards for law enforcement and the judiciary. Significantly, in paragraph 60 it states that any measures to eliminate online violence against women must comply with international human rights law, including the criteria for permissible restrictions to freedom of expression provided under Article 19(3) of the International Covenant on Civil and Political Rights (ICCPR). It calls for a multifaceted approach to addressing online violence against women:

- Preventive (including education and technical features, for example)
- Reactive (swiftly take down unlawful content, and investigate)
- Redress for victims.

It notes various approaches that states are taking, but calls out states, law enforcement agencies and courts for "failing to take appropriate action in situations of online violence against women, or [...] using such laws as a pretext to restrict freedom of expression." There was also a strong emphasis that efforts to address online violence against women must be consistent with Article 19(3) of the ICCPR.

These developments culminated in the Committee on the Elimination of Discrimination against Women (CEDAW) General Recommendation No. 35,[44] which makes extensive reference to online gender-based violence (despite not using this actual terminology), including the following:

> Gender-based violence against women occurs in all spaces and spheres of human interaction, whether public or private. These include the family, the community, the public spaces, the workplace, leisure, politics, sport, health services, educational settings and their redefinition through technology-mediated environments, such as contemporary forms of violence occurring in the internet and digital spaces. In all these settings, gender-based violence against women can result from acts or omissions of State or non-State actors, acting territorially or extraterritorially, including extraterritorial military action of States,

[42] A/HRC/RES/34/7, available at: undocs.org/A/HRC/RES/34/7

[43] A/HRC/35/9, available at: ap.ohchr.org/documents/dpage_e.aspx?

[44] Committee on the Elimination of Discrimination against Women. (2017). General recommendation No. 35 on gender-based violence against women, updating general recommendation No. 19. tbinternet.ohchr.org/Treaties/CEDAW/Shared%20Documents/1_Global/CEDAW_C_GC_35_8267_E.pdf

individually or as members of international or intergovernmental organizations or coalitions, or extraterritorial actions by private corporations.[45]

Given this definition of all spheres specifically mentioning technology-mediated environments, this can be used to push for states to take legislative and policy measures to address online GBV as part of their obligations under CEDAW.

As demonstrated, the past decade has seen significant developments in relation to understanding and recognising online gender-based violence within the global UN system. It is important to note that this recognition, however, is not only related to the role of the state, but also the private sector, which is a critical actor in developing effective prevention and response mechanisms.

4. Key issues for consideration

4.1. Tensions between rights[46]

Tensions around multiple rights are often raised in discussions on online gender-based violence, as states have responded to calls for action with conservative, often moralistic, protectionist measures which, for example, can have the consequence of censoring or limiting speech. APC and other women's rights advocates have responded by stating that online violence in effect curtails women's right to freedom of expression, public participation and privacy by creating a hostile and unsafe online environment that can result in women withdrawing from online spaces.

Similarly, while anonymity and the protection of privacy are vital for the exercise of freedom of expression online, including the right of women to access critical information and support services, and for whistle-blowers, these rights may also help to enable GBV by providing perpetrators with a cloak of invisibility and, thus, perceived impunity. Many governments have argued that surrendering or diminishing the right to privacy and anonymity is necessary to ensure safety. It is therefore ironic that women and communities most at risk of discrimination, historically subject to social surveillance, scrutiny and control of mobility in societal efforts to enforce established gender roles, now are told they must endure state surveillance in order to "keep them safe". In addition, APC's research found that the majority of online GBV was committed by someone known to the victim/survivor.

Measures that protect women online must consider multiple rights, including the right to safety, movement, to participate in public life, freedom of expression, and privacy, among others, and must take into account existing inequalities and discrimination which may affect how rights are protected and recognised. In considering any restriction on these rights, states need to consider the importance, nature and extent of any limitation proposed and should opt for the least restrictive means to achieve that purpose. This is particularly essential in a global context of closing civil society spaces and the development and implementation of laws and policies which reveal a backlash against the gains made in relation to women's rights more generally.

[45]Emphasis added.

[46]This section draws extensively on the report of the IGF 2015 Best Practice Forum on Online Abuse and Gender-Based Violence Against Women.

4.2. Internet intermediaries

The role of internet intermediaries has increasingly come under the spotlight in relation to the governance and regulation of the internet. This is because online gender-based violence is transmitted through privately owned platforms that are often operating in many jurisdictions. Given the inadequate response of law enforcement, many victims/survivors often turn to social media platforms to seek remedy. While a great deal of attention has been placed on the business and human rights practices of intermediaries, there has been less attention paid to how their policies and practices impact specifically on communities outside of the US where the majority of social media platforms used by victims/survivors are based.

APC research demonstrates that poor responses from intermediaries in relation to online GBV can contribute to the chilling effect on expression mentioned previously, with terms of service that can lead to censorship by platforms, other users (through reporting), or self-censorship, without actually providing the targets of harassment with redress or recourse, especially for those in non-English-speaking countries.

APC conducted research assessing existing company policies to shed light on best practices and possible solutions to women's demands for corporate accountability. Twenty-four case studies were conducted across seven countries and 22 company policies were reviewed in 2014.[47] We found that:

- Recognition of human rights: Only two of the 22 companies reviewed have a formal commitment to human rights.
- National telephony companies: No company reviewed names threats of physical or sexual violence as prohibited behaviour in their terms of service.
- Social media platforms: The companies fail to engage with the perspectives of women outside of North America or Europe.
- Pornography websites: The use of pornography websites for the non-consensual distribution of content is widespread.
- Legal liability: The terms of service are often only a reflection of the company's legal obligations in its country of residence (such as with regard to copyright infringements).

Informed by this research, APC sees a need to move beyond the discussion of liability and towards one of responsibility. Liability denotes a restrictive approach that endangers the free and open nature of the internet and implies a risk-based consideration; responsibility infers a role defined by empowerment, positive action, and leadership. Therefore, we recommend promoting the important role of intermediaries in fostering positive attitudes and accountability online in a way that does not lead to state manipulation or co-option.[48]

This is in line with Article 17 of the Council of Europe's Istanbul Convention,[49] which recognises the important role that the media can play to fight against gender discrimination and contribute to the

[47]Athar, R. (2014). *From impunity to justice: Improving corporate policies to end technology-related violence against women*. Association for Progressive Communications. https://www.genderit.org/sites/default/.../flow_corporate_policies_formatted_final.pdf

[48]Nyst, C. (2013, 26 November). Towards internet intermediary responsibility. *GenderIT.org*. www.genderit.org/feminist-talk/towards-internet-intermediary-responsibility

[49]Council of Europe Convention on preventing and combating violence against women and domestic violence, available at: https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=090000168046031c

freedom of expression of women, who often opt not to participate in public debate due to the misogynistic speech and online harassment they face online. The Convention calls on the private sector to set guidelines to prevent violence against women and to enhance respect for their dignity. It also calls on states to cooperate with the private sector to develop educational programmes for users on how to deal with degrading online content of a sexual or violent nature which might be harmful.

Internet intermediaries are motivated by profit and respond to different platform objectives and terms of service for their communities, depending on the type of community and online experience they hope to foster. In an era where the best capture and analysis of individuals' data determines better advertising income, the right to privacy is particularly affected. Privacy is further eroded by data searchability and persistence. The possibility of censorship and government awareness of who is expressing particular speech due to precise user location, data interconnection, and real name enforcement are other concerns expressed by freedom of expression advocates.

In order to operate in different national and regional markets, companies have installed backdoors[50] or applied more restrictive privacy controls due to national legislative requirements.[51] On the one hand, concessions to operate in a particular national context put into question the security of customer communication, especially if there is no third party testing or transparency report regarding concessions made, and open the door to government censorship and abuse of human rights with an ability to target specific communities, such as LGBTIQ communities. On the other, companies have shown that increased and facilitated customer control over individual privacy is indeed possible, but largely only made available in scenarios of forced compliance.[52]

Feminist activists denouncing rights violations or doing educational and advocacy work, especially regarding sexual rights, have seen their communications channels regularly targeted through social network reporting mechanisms which result in temporary or permanent account closure. In contrast, when women report the dozens to hundreds of comments attacking them and burying their message on platforms, they are told that threats and other violent content are not against community standards, suggesting an inherent sexist bias in either support staff or company policies. Furthermore, any display of women's naked bodies is frequently interpreted in company terms of service and by other users (seeking to silence feminist expression) from a moralist point of view that automatically sexualises the female body for the male heterosexual gaze. Censoring women's representations of their own bodies denies women's right to political, creative, sexual and other expression through embodiment. Social networking platforms, given their ubiquity, increasing user base and contradictory enforcement of terms of service, play an important role of normalising gender-based violence and reducing women's bodies to sexual objectification.[53]

---

[50]See, for example: Whittaker, Z. (2013, 8 March). 1,168 keywords Skype uses to censor, monitor its Chinese users. *ZDNet*. https://www.zdnet.com/article/1168-keywords-skype-uses-to-censor-monitor-its-chinese-users; Mozur, P., Scott, M., & Isaac, M. (2017, 17 September). Facebook faces a new world as officials rein in a wild web. *The New York Times*. https://www.nytimes.com/2017/09/17/technology/facebook-government-regulations.html

[51]See, for example: Kayyali, D. (2015, 26 February). New report shows European data protection authorities are taking Facebook's questionable terms of service seriously. *Electronic Frontier Foundation*. https://www.eff.org/es/deeplinks/2015/02/new-report-shows-european-data-protection-authorities-are-taking-facebooks

[52]See, for example: Schechner, S. (2015, 2 April). Facebook Privacy Controls Face Scrutiny in Europe. *Wall Street Journal*. https://www.wsj.com/articles/facebook-confronts-european-probes-1427975994

[53]See, for example: Datta, B. (2014, 16 September). Never mind the nipples: Sex, gender and social media. *GenderIT.org*. https://www.genderit.org/es/node/4149; Pasricha, J. (2016, 10 November). It's 2016 and Facebook is

APC's research found that platform policies and solutions do not adequately reflect proper consultation with affected communities, especially non-English-speaking women from the global South, with little recognition or understanding of the specific experiences of women and groups at risk of injustice. It should be noted, however, that some of the larger social networking services are beginning to engage with women's rights organisations and have been carrying out regional consultations and other convenings to solicit input. Nevertheless, overall, companies still appear reluctant to report how much information is being flagged and taken down and under what criteria.[54] There is also still limited transparency in decision making and application of community standards to ensure that gender-based violence on platforms is more easily reported and being swiftly addressed.[55]

4.3. Freedom of expression[56]

A 2015 report on the status of freedom of expression in Norway notes:

> Hate speech contributes to social exclusion and increased polarisation. Moreover, such speech intimidates people and deters them from speaking publicly; thus weakening democracy. Hate speech fans prejudice, creates fear and anxiety among the affected groups, and deprives people of dignity. Hate speech can therefore trigger discrimination and harassment and/or violence.[57]

APC's research reflects this, and shows how online gender-based violence has a chilling effect on women's speech, and as such, is a key issue in relation to freedom of speech more generally.

The report from Norway further notes:

still terrified of women's nipples. *GenderIT.org*. https://www.genderit.org/feminist-talk/its-2016-and-facebook-still-terrified-womens-nipples; Chemaly, S. (2014, 22 April). Why female nudity isn't obscene, but is threatening to a sexist status quo. *Huffington Post*. https://www.huffingtonpost.com/soraya-chemaly/female-nudity-isnt-obscen_b_5186495.html; Gibbs, S. (2017, 5 December). Facebook bans women for posting 'men are scum' after harassment scandals. *The Guardian*. https://www.theguardian.com/technology/2017/dec/05/facebook-bans-women-posting-men-are-scum-harassment-scandals-comedian-marcia-belsky-abuse. It should be noted that in accompanying women seeking take-down of intimate material from do-it-yourself pornography sites, we have noted in such sites the striking difference between their terms of service regarding privacy and consent versus their advertising and uploading forms which urge contributors to cite age, names and geographic locations with no mention of consent.

[54]In an August 2017 joint statement on Facebook's internal guidelines for content moderation, APC and a number of its members and partners observe that the company's limited consultation with women's rights groups and activists "has not been meaningful enough to create real change. Often, learnings from these interactions appear to stay with the company representatives present, as we have repeatedly experienced that one arm of the company does not talk to the other." The statement also notes that Facebook's policies still fail to reflect a full understanding of gender-based violence: "One glaring issue is the use of the term 'credible violence', akin to the popularly derided term 'legitimate rape', which in itself perpetuates violence." Finally, the statement emphasises the free labour that organisations like APC give to these companies in working through individual cases because of lack of systemic change. "We should not have to do Facebook's work for them." The statement is available at: https://www.takebackthetech.net/news/joint-statement-facebooks-internal-guidelines-content-moderation

[55]For more details, see, for example: Leidel, S. (2015, 12 November). Tech companies fail to make the grade on privacy. *Deutsche Welle*. www.dw.com/en/tech-companies-fail-to-make-the-grade-on-privacy/a-18844921; and Ullman, I. (2017, 23 March). The Ranking Digital Rights 2017 Corporate Accountability Index is now online! *Ranking Digital Rights*. https://rankingdigitalrights.org/2017/03/23/2017-index-now-online

[56]This section draws extensively on the report of the IGF 2015 Best Practice Forum on Online Abuse and Gender-Based Violence Against Women and Nyst, C. (2013, 26 November). Pulling back the veil of free speech. *GenderIT.org*. https://www.genderit.org/feminist-talk/pulling-back-veil-free-speech, as well as APC's 2016 submission to the Special Rapporteur on freedom of opinion and expression's report on the private sector and freedom of expression in the digital age, available at: https://www.apc.org/en/pubs/freedom-expression-and-private-sector-digital-age

[57]Ørstavik, S. (2015). *The Equality and Anti-Discrimination Ombud's Report: Hate Speech and Hate Crime*. https://www.genderit.org/sites/default/upload/hate_speech_and_hate_crime_v3_lr.pdf

> Groups that are already exposed to other forms of discriminatory behaviour will experience being subjected to hate speech in public as more stressful than individuals and groups who, to little or no extent, are subjected to discriminatory behaviour. From such a perspective, efforts against hate speech will also be an important contribution to the fight against discrimination and for equality. Furthermore, by reducing the extent of hate speech, it will promote real freedom of expression for those who currently choose not to participate in public debate.

While the right to freedom of expression is guaranteed by Article 19 of the International Covenant on Civil and Political Rights, it is not, however, an absolute right. A person cannot say and communicate whatever they would like without concern or consideration for the enjoyment of others' human rights. Restrictions on the right to freedom of expression must be provided by law, and be necessary for respect of the rights or reputations of others, or for the protection of national security or of public order, or of public health or morals (Article 19(3)). Moreover, freedom of expression cannot be used to justify language or other forms of expression designed to incite discrimination, hostility or violence (Article 20 (2)).

Legal definitions of hate speech vary dramatically among countries, putting in dispute a globally accepted definition. They do seem to coincide on gender: generally speaking, legal frameworks do not consider incitement to gender-based violence as hate speech.

Nonetheless, given that violence against women has been recognised as being a manifestation of historically unequal power relations between men and women, and an obstacle to the achievement of equality, development and peace, it follows that incitement to violence, discrimination and hostility against/towards women and gender-based violence fall within the exception to freedom of expression.

However, the existence of exceptions to the right to freedom of expression does not mean that the prohibition against hate speech and incitement to hatred is a straightforward or uncontroversial idea. To the contrary, the exceptions to Article 19 are highly controversial, subjective and prone to manipulation by state entities. This is particularly the case when talking about hate speech on the internet. So, whereas many states have now prohibited hate speech in the mainstream media and provided avenues for legal address, including civil, administrative and criminal measures, addressing and redressing hate speech on the internet remains a complex process, and one which in many circumstances has opened the door for greater state repression and curtailment of free expression rights.

In this context, the 2011 report of Special Rapporteur on freedom of opinion and expression Frank La Rue,[58] referenced earlier, noted that states have taken steps to implement a number of impermissible restrictions on the right to freedom of expression in the name of curtailing hate speech. These include the blocking or criminalisation of content related to discussion of government policies and political debate, reporting on human rights, government activities and corruption in government; engaging in election campaigns, peaceful demonstrations or political activities, including for peace or democracy; and expression of opinion and dissent, religion or belief, including by persons belonging to minorities or vulnerable groups. Any permissible state initiative to block content must, according to the Special

[58] A/HRC/17/27.

Rapporteur, be content-specific, and must be authorised by an unambiguous law, pursue a legitimate purpose, and respect the principles of necessity and proportionality.

This would also include content related to online gender-based violence, as was further emphasised by the joint statement[59] issued by the Special Rapporteur on violence against women and the Special Rapporteur on the promotion of freedom of expression on 8 March 2017, which focused on the need for holistic preventative measures as well as the necessity of swift response, in collaboration with internet intermediaries:

Apart from preventive measures women victims and survivors need transparent and fast responses and effective remedies which can only be achieved if both States and private actors work together and exercise due diligence to eliminate online violence against women.

4.4. Anonymity and encryption

Anonymity is fundamental for the full exercise of the right to freedom of expression, as enshrined in Article 19 of the Universal Declaration of Human Rights and the International Covenant on Civil and Political Rights. As former UN Special Rapporteur on freedom of opinion and expression Frank La Rue notes, "throughout history, people's willingness to engage in debate on controversial subjects in the public sphere has always been linked to possibilities for doing so anonymously."[60]

Historically, leaflets or pseudonyms in the press enabled anonymous speech. Anonymity is especially critical in repressive environments in which certain types of protected expression are outlawed, and lack of anonymity could lead to criminal charges or other consequences.

The ability to be anonymous online has fulfilled an important function for women and others at risk of discrimination because it has allowed them to seek information, find solidarity and support and share opinions without fear of being "found out". In particular, individuals such as those who face discrimination and persecution based on their sexual orientation and gender identity, and/or those experiencing gender-based violence, may be forced to rely on encryption and anonymity in order to circumvent restrictions and exercise the right to seek, receive and impart information.

APC conducted exploratory research on sex, rights and the internet,[61] examining how the internet facilitates the exercise of sexual rights and the expression of sexualities, particularly of women living in different socio-political, economic and cultural contexts, and how emerging regulation online affects this ability. Our research found that:

> Due to the interactivity and anonymity facilitated by internet technology, the targets of hate speech and online harassment may engage in direct verbal interaction with their aggressors. Rather than acting as passive victims, the former have the opportunity to exercise effective responses.

At the same time, perpetrators often use anonymous accounts in perpetuating abusive behaviour and violations online. This presents a challenging context for addressing the issue of online violations of

[59] www.ohchr.org/EN/NewsEvents/Pages/DisplayNews.aspx?NewsID=21317&LangID=E

[60] A/HRC/17/27.

[61] EROTICS: An exploratory research project into sexuality and the internet. https://www.apc.org/en/projects/erotics-exploratory-research-project-sexuality-and-0

women's rights while balancing other fundamental rights. To address the issue, David Kaye, the UN Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, noted during the Best Practice Forum session at IGF 2015 that the "default option" for technologies should be anonymity, followed by an investigation of the problems that anonymity may cause.

Kaye's 2015 report on encryption and anonymity[62] highlights that individuals, such as those who face discrimination and persecution based on their sexual orientation and gender identity, may be forced to rely on encryption and anonymity in order to circumvent restrictions and exercise the right to seek, receive and impart information. Importantly, the report contends that anonymity, including conducting and saving searches anonymously, is fundamental for the full realisation of the right to develop and hold opinions.

Yet despite evidence that shows how important anonymity and encryption are, a 2016 report by UNESCO[63] notes that "much of the debate about encryption has, until now, been gender-blind, or perhaps worse, male-dominated." In a context of increasing levels of online gender-based violence, and shrinking spaces for people of diverse sexualities to organise and build solidarity, it is essential that these debates reflect the concerns of these communities.

One particularly harmful example of not consulting with affected communities was painfully demonstrated with Facebook's 2015 real-name policy imposition, which automatically and dangerously exposed transgender people, activists and survivors of domestic violence, even with belated remedies to address at-risk communities.[64]

4.5. Concerning legislative and judicial responses

As noted, APC's research found that women's access to justice in cases of gender-based violence online was frequently limited due to inflexible interpretation of existing legislation addressing GBV, data privacy and cybercrime. There is increasing pressure on legislators to develop new legislation which could roll back hard-won guarantees such as the decriminalisation of defamation. Persuasive survivor lobby groups will often call for remedies that effectively entail prior censorship and invasion of privacy, which find an echo in government interests to eliminate anonymity and gain access to private communications in the name of national security.

Offensive, discriminatory and even violent commentary may create an enabling environment for GBV, but in and of itself should not be subject to imprisonment. Furthermore given patriarchal and racist judicial systems where impunity is more common than justice, there is the possibility of new laws being used against those vulnerable communities it was designed to protect. New bills frequently propose harsh jail sentences which do not seem to compare to suggested punishment under existing GBV legislation.

One area of new legislation emerging in many countries is regarding the non-consensual dissemination of intimate images, which is also sometimes linked to acts of extortion to obtain more intimate material or carry out sexual violence. This type of legislation is concerning on many levels.

---

[62]A/HRC/29/32, available at: https://undocs.org/A/HRC/29/32

[63]Schulz, W., & van Hoboken, J. (2016). *Human Rights and Encryption*. UNESCO. unesdoc.unesco.org/images/0024/002465/246527E.pdf

[64]APC et al. (2015). Open Letter to Facebook on Real Name Policy. https://www.apc.org/en/pubs/open-letter-facebook-real-name-policy

First, non-consensual distribution of intimate content is commonly referred to as "revenge porn", a misnomer which simultaneously applies implicit blame to the victim/survivor, ignores a full range of aggressors, and invokes a moralist reaction. Citing that an action is the result of "revenge" implies that the aggressor was provoked by an inappropriate action of the victim, that they were somehow responsible or could have avoided it. It further puts this type of violence into a two-person intimate partner relationship, ignoring the many motives and points of access and distribution possible, thus limiting the possibility of redress or application of sanction to others involved. Furthermore, it assumes that the material is pornographic, which is defined differently in each country's national legislation, but in theory is a specific commercial relationship based on consent, which is not reflected in the majority of cases of non-consensual distribution. Pornography and voluntary sexual content production is frequently received from a moralistic, heteronormative standpoint and those who participate in it can be subject to harsh societal judgement.

Another misnomer applied to the non-consensual distribution of intimate content is the practice or concept of "sexting", which several local entities or even national law have now incorporated into their criminal codes, effectively criminalising sexual expression between consenting adults, and in some cases confounding teen sexuality with images of child sexual exploitation.

The debate around non-consensual distribution of intimate content also puts understandings around consent and image ownership into question. Consensual exchange of photos in an intimate relationship does not necessarily transfer consent and decision-making authority regarding redistribution, storage or reuse of that material. There are no clear avenues to ensure revocation or time-bound determination of consent and compliance.

Furthermore, one might voluntarily upload erotic content for public online consumption, without revealing identity, not expecting that due to searchability and data trails others might eventually associate and promote the material linking directly to their names, addresses, etc., increasing risk of harm.

In the case of online intimate content, legislation and private sector policies suggest that "risky" behaviour implies responsibility and are therefore weak or fatalistic on solutions and responsibility of others involved. For example, Google will not de-index intimate content that a person voluntarily uploaded anonymously, although that content is now automatically associated with that person due to Google's efficient search algorithms.

Governments tend to prioritise legislative solutions, but they take time and are frequently already outpaced by technology – and online gender-based violence practices – upon passage. Adapting existing gender-based violence and cybercrime legislation, or opening interpretation to encompass technology-related gender-based violence, may be more practical than creating new legislation.

Our research found that instead of focusing on the violence exercised and resulting harm, officials would refuse to file women's reports of abuse or matters were dismissed in the courts because they could not find a corresponding crime or violation in the penal or civil code which specifically cited the information and communication technologies in question. Knowledge about what information can be requested of internet intermediaries in a police investigation and appropriate, swift protocols are frequently absent in both existing and new legislation.

Some legislative responses bypass recognised standards for due process or have put the burden of responsibility for investigation of individuals and content take-down on internet intermediaries and entire platforms, surpassing a necessary and proportionate response to curb gender-based and other violence.[65]

Solutions in this example need to be swift and holistic and in cooperation with private sector platforms to avoid increased harm. As the Best Practice Forum report[66] cites:

> Governments should also ensure that they facilitate and simplify access to justice for survivors whilst prioritising redress and relief over criminalisation. Where possible, governments should consider options beside traditional courts and tribunals. The creation of specialised, fast-track courts or specialised agencies to investigate complaints can, for instance, help to provide simple, quicker and more cost-effective (especially in comparison to ordinary courts) forms of recourse to victims.

APC's research found that swift redress like protection orders and clear take-down protocols (following due process) were preferred over criminalisation, which can result in lengthy judicial proceedings, lawsuits that do not amount to any damages paid, reliving trauma or even bringing more attention to the concerning content in the first place.

5. Recommendations

The thematic report is a significant contribution towards developing effective responses by state and non-state actors to online gender-based violence and providing adequate relief and remedy for victims/survivors. While the areas for intervention are many, we focus on the following recommendations for policy makers and do not provide extensive recommendations for intermediaries, given the focus of the report:

1. Elaborate on and further develop a comprehensive definition of online gender-based violence which reflects both the continuum of violence and the common root causes as well as the particular experiences of victims/survivors made possible through the unique specificities of digital technologies.
2. Ensure that legal frameworks adequately protect women's freedom of expression (including political, religious and sexual expression), privacy, and freedom from violence. Any restrictions to freedom of expression to respond to gender-based violence and abuse must be necessary and proportionate, should not be overbroad or vague in terms of what speech is restricted, and should not overpenalise (whether referring to criminal sentencing or responses which restrict internet or platform access).
3. Morality and obscenity as rationale for protecting women and other communities affected by injustice must not be the basis for any legislative reform or new law in matters of gender-based

[65] See, for example: Meyer, D. (2016, 20 July). Supreme Court Gives WhatsApp Back to Millions of Brazilians. *Fortune*. fortune.com/2016/07/20/whatsapp-brazil-unblocked; Dhapola, S. (2016, 30 June). Supreme Court rejects PIL for WhatsApp ban, but encryption debate is just beginning. *Indian Express*. indianexpress.com/article/technology/tech-news-technology/supreme-court-rejects-pil-for-whatsapp-ban-but-encryption-debate-is-just-beginning-2885121

[66] https://www.intgovforum.org/cms/documents/best-practice-forums/623-bpf-online-abuse-and-gbv-against-women/file

violence online. Any law must foreground rights to bodily autonomy, self-determination, freedom of expression and rights to participate in public debate.

4. States should not suppress anonymity or encryption. Survivors often need this to re-enter online spaces, to feel safe, to share their stories and to find information. There are other ways to find the perpetrators.
5. Adaptation of existing law, or flexible interpretation to encompass technology-related GBV, may be more practical than time-consuming creation of new legislation.
6. Governments should ensure that they facilitate and simplify access to justice for victims/survivors while prioritising reparation and redress over criminalisation. Means of swift redress could include specialised, fast-track courts or agencies to investigate complaints, able to accept third-party complaints and to act both reactively, in response to specific complaints, and proactively, in response to potential trends; issuance of protection orders, emergency take-down protocols which still follow due process, etc.
7. Law creation or reform regarding the regulation of the internet must involve extensive consultation with women's rights and sexual rights civil society organisations to ensure synergy with other legislative developments responding to online GBV and to integrate a gendered awareness into potential measures to avoid any discriminatory effect.
8. Training for law enforcement, judiciary and other response actors to take GBV online seriously and react swiftly, through deepening their understanding of technology and how it can facilitate and exacerbate violence, sensitising them against victim blaming and moralistic reactions, outlining protocols to request take-down and/or obtain information from internet intermediaries following due process, etc.
9. Legislative reform and/or new legislation regarding online GBV in and of itself is not sufficient. Holistic solutions for online GBV prevention and response should include both legal and non-legal measures, such as improving access, digital literacy, the creation of enabling environments for diverse expressions, as well as clear and specific delineations of legal and illegal gender-based hate speech.
10. Responses to and prevention of online GBV should strive to create an enabling environment for women's access to and enjoyment of ICT in terms of quality infrastructure, training in highly technical skills, and meaningful participation in internet governance for women.
11. Internet intermediaries should be encouraged to ensure data security and privacy by design,[67] embedding privacy as the default option of their services and considering all user data as sensitive information.
12. Internet intermediaries have the responsibility to respect human rights, including preventing gender-based violence, on their platforms. This includes but is not limited to conducting due diligence and providing remedy and redress. Government regulation and imposition of obligations on internet intermediaries should also respect the human rights framework, employing necessary and proportionate measures.

[67]Cavoukian, A. (2011). *Privacy by Design: The 7 Foundational Principles*. https://www.ipc.on.ca/wp-content/uploads/Resources/7foundationalprinciples.pdf