APC ISSUE PAPERS

DUE DILIGENCE AND ACCOUNTABILITY FOR ONLINE VIOLENCE AGAINST WOMEN

*By Zarizana Abdul Aziz (Due Diligence Project)**

KEYWORDS: **due diligence, online violence against women, consent, human rights, state, internet intermediaries, international law**

SUMMARY

This paper explores what online violence against women is; what can be done to stem and ultimately eliminate it; and whose responsibility it is to do so. It does this by building upon the issues identified in two research projects, namely the research on state accountability to eliminate violence against women by the Due Diligence Project (DDP)[1] and the research on corporate and state remedies for dealing with online violence against women by the Association for Progressive Communications (APC).[2]

The paper further looks at the roles played by both states and private corporations as well as the legislative and non-legislative changes that are needed to ensure that women are able to exercise their right to freedom of expression without fear of harassment or violence. It recommends that innovations in other fields of online

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

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

* Zarizana Abdul Aziz is a human rights lawyer and the director of the Due Diligence Project, and co-developed the Due Diligence Framework on State Accountability for Eliminating Violence against Women.

This paper was produced in collaboration with the Due Diligence Project. The views expressed in this paper do not necessarily represent the position of APC, but they do represent the opinions, experiences and thoughts of the authors, and that makes them extremely valuable. To read more on this subject, please visit www.genderit.org/onlinevaw

APC
ASSOCIATION FOR PROGRESSIVE COMMUNICATIONS

jurisprudence could provide a template for addressing gender-based violence online.

KEY CONCEPTS

Online violence against women: Acts of gender-based violence "committed, abetted or aggravated" in part or fully by the use of information and communication technologies (ICTs), such as cyber stalking; accessing or disseminating a woman's private data (through hacking); identity theft or doxxing.

Due diligence: International law mandates states to exercise due diligence 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. This also includes the obligation to remove impunity and prevent human rights abuses by non-state actors. Non-state actors include transnational[3] and national corporations operating within the jurisdiction of the state.

Internet intermediaries bring together or facilitate transactions between third parties on the internet. They give access to, host, transmit and index content, products and services originated by third parties on the internet or provide internet-based services to third parties.

Intermediary liability in the context of this paper refers to the legal liability of internet intermediaries for content contributed by, or activities carried out by, third parties. The liability approach this paper pursues is "notice and takedown" systems, i.e. systems that require intermediaries to act expeditiously to remove content which is deemed to be unlawful once they have been given notice of the content to ensure that their sites do not serve as vehicles for violating material. Such takedown orders should be issued by a judicial authority, be clear and unambiguous, and follow due process.

KEY FACTS

- Online violence against women presents specific challenges in gauging which data or images constitute violence. What is actionable violence and what is not is gauged by intent to harm, content, imminence of harm (credibility), extent of the harm and context.
- ICT provides a fertile terrain that amplifies reach of transmission. This aggravates the harm to the exercise and enjoyment of human rights and freedoms, particularly the right to privacy or respect for private life caused by the communication of the violating material compared to more traditional media.
- Patriarchy and prevailing interpretations of moral norms, culture and religion situate women as the primary bearers of honour and tradition. Women who establish cyber-friendships or relationships may be deemed to have transgressed culturally appropriate behaviour, as are women who engage in sexting, exchanging images or who consent to intimate partners taking suggestive images, albeit for private purposes.
- In relation to violence against women, consent is key to differentiating lawful from unlawful and harmful behaviour. Consent in an online context is often complicated by the exact act to which the consent, if any, relates. Because of this, defining consent is crucial in online violence and must be addressed in any relevant mechanisms.
- The enhanced anonymity offered by digital and virtual spaces, through encryption and privacy protocols, provides particular challenges in identifying perpetrators of online violence against women and magnifies impunity.
- It is simplistic to view anonymity as a threat that needs to be removed under all circumstances. Anonymity offers privacy to victims/survivors (whose privacy is often violated by perpetrators) and allows them to re-enter online spaces or to report violence. The anonymity provided by the internet is also beneficial to whistleblowers, human rights defenders, and those outside current dominant groups, such as LGBTIQ people.

INTRODUCTION

Increased prevalence of online violence against women, the lack of effective measures to prevent and contain it, and the ensuing impunity must be addressed as part of the struggle to eliminate all forms of gender-based violence. Online information and communications technologies are often the main form of communication in commercial dealings as well as personal, political and social interaction. This makes eliminating online violence against women increasingly critical.

3 Transnational corporations are companies that operate across borders. This raises challenges in terms of the regulating country (where the harm of the crime arose).

The internet, once a liberating space, is also, increasingly, a space of violence, particularly violence targeting women. While it is beyond the scope of this paper to explore why women are targeted within online spaces, online violence against women is part of the continuum of violence against women that is committed offline. It reflects and parallels the reality of offline violence against women with the same causes and similar consequences. Like offline violence against women, internet-related violence against women is often in the form of sexual violence such as threats of rape, non-consensual dissemination of intimate data and images, dissemination of rape recordings, cyber stalking, sexual harassment and the exploitation of women and girls.[4]

Another group of persons susceptible to online violence is the LGBTIQ community. In so far as its form, frequency and severity can be compared to approximate the form, frequency and severity of online violence against women, this paper is equally applicable to addressing and eliminating violence against LGBTIQ persons.

Freedom of expression and access to information are key enabling rights to a range of human rights. Online violence prevents women and girls from fully exercising these rights. Thus, removing violence against women from digital and online platforms has the net effect of promoting and strengthening freedom of expression as it creates an environment that allows more individuals, especially sections of society who face discrimination in other public spaces, to participate in these media.[5]

Initiatives by states and internet intermediaries to confront online violence have proven ineffective in stemming online violence, protecting women, bringing the perpetrators to account or providing satisfactory redress for victims/survivors. In her September 2016 report, the United Nations Special Rapporteur on violence against women, its causes and consequences, Dubravka Šimonović, identified online violence as a new challenge and one of her priority issues:

> While the use of information and communications technology has contributed to the empowerment of women and girls, its use has also generated online violence. … [T]here is a need to examine this recent phenomenon, and the applicability of national laws to it, and to make recommendations for states and non-state actors to fight online violence against women and girls while respecting freedom of expression and the prohibition of incitement to violence and hatred, in accordance with article 20 of the International Covenant on Civil and Political Rights.[6]

This paper explores what online violence against women is; what can be done to stem and ultimately eliminate it; and whose responsibility it is to do so. It does this by building upon the issues identified in two research projects, namely the research on state accountability to eliminate violence against women by the Due Diligence Project (DDP)[7] and the research on corporate and state remedies for dealing with online violence against women by the Association for Progressive Communications (APC).[8]

OUTLINE OF PAPER

The paper outlines women's experiences in accessing justice; identifies and describes the issues, actors and stakeholders; the role of the state as well as private sector actors; existing mechanisms; application of international human rights law; and good or promising practices in this context. It concludes with recommendations.

The first part will look at violence against women in general and the ability of technology to amplify violence against women. Technology provides platforms capable of masking perpetrators as well as allowing perpetrators to commit violence at increased distance, speed and rate. The capacity of technology to store data and images complicates the provision of remedies.

The second part looks at actors and stakeholders. The primary actor is the perpetrator, namely the originator (author) of the online violence. Layers of encryption

4 Association for Progressive Communications. (2014). *Analysis of incidents of technology-related violence against women reported on the "Take Back the Tech!" Ushahidi platform.* www.genderit.org/onlinevaw

5 A 2015 report on the status of freedom of expression in Norway cites the Norwegian survey on the status of freedom of speech from 2014 that "shows that hate speech can have harmful effects for those who participate in public debate. In the survey, it emerges that the harm is greater among people with ethnic minority backgrounds than those with majority background." It further notes that "there is no reason to assume that the same harmful effects don't also apply to other groups who are particularly vulnerable to hate speech related to actual or perceived personal characteristics." The report also documents that such speech intimidates people and deters them from speaking publicly. See Ostavik, S. (2015). *The Equality and Anti-Discrimination Ombud's Report: Hate speech and hate crime*. www.genderit.org/sites/default/upload/hate_speech_and_hate_crime_v3_lr.pdf

6 Šimonović, D. (2016). Report of the Special Rapporteur on violence against women, its causes and consequences (A/HRC/32/42). https://documents-dds-ny.un.org/doc/UNDOC/GEN/G16/080/53/PDF/G1608053.pdf?OpenElement

7 Abdul Aziz, Z., & Moussa, J. (2013). Op. cit.

8 Association for Progressive Communications. (2015). Op. cit.

allow the perpetrator to remain anonymous. Further, any post can be distributed or accessed online, drawing secondary transmitters who unwittingly or knowingly amplify the harm to the victim/survivor.

Platform providers and intermediaries often deny liability or even responsibility to ensure that their sites do not serve as vehicles for violations. This complicates victims'/survivors' ability to obtain remedy, which requires the cooperation of these intermediaries.

The third part dissects what constitutes infringement. How do we differentiate between the legitimate exercise of freedom of expression and violence? The issue of expression in the face of harm has been dealt with in other areas that may prove helpful in defining infringement in cases of violence against women.

The fourth part looks at the application of international law and issues of accountability for online violence, exploring international law's contribution toward resolving online violence. This paper will also interrogate whether it is appropriate and feasible to hold internet intermediaries accountable for failure to prevent, respond to and provide remedy for online violence against women committed on their platforms.

As internet intermediaries can only be held accountable if they have a positive obligation in this regard, the paper will explore whether it is possible to imbue internet intermediaries with a positive obligation to exercise due diligence in these instances. Issues such as anonymity and extraterritoriality complicate states' prosecuting or holding perpetrators or third parties liable. Still, states are not exempt from discharging their obligations on the basis that the wrong is difficult to investigate or prosecute.

The fourth part also interrogates the role of the state to exercise due diligence to prevent online violence, protect victims/survivors, investigate and prosecute instances of online violence, punish perpetrators and provide redress to victims/survivors.

The fifth part interrogates what measures states have undertaken in addressing online violence and whether these actions, policies, laws and programmes are effective. While many states have attempted to criminalise online violence, enforcement has proven seriously problematic due to lack of mechanisms, procedures and expertise/skills. As the violating material is posted on a third party platform, often sited beyond the territorial limits and jurisdiction of the state concerned, providing remedies and reparation to the victim/survivor has proven especially difficult. Takedown notices, removal of links and disclosure of identity can only be undertaken by third parties who may or may not be liable for the violating material posted on their platforms.

Finally, the sixth part explores ways forward and outlines recommendations and principles to address online violence.

DEFINITION, GAPS AND CHALLENGES

This part looks at four issues. First, it discusses online violence against women and its manifestations, as well as drawing parallels to offline violence against women. It then looks at stigmatisation of the victim/survivor. Not only are victims/survivors blamed for the violence committed against them, but also, because the violence is not "physical", state authorities and private sector players, such as internet intermediaries, tend to minimise its perceived gravity.

The third issue is how online VAW aggravates harm. Online violence is facilitated by instantaneous transmission through vast digital networks. Once uploaded, it may remain online permanently. Finally, this part discusses the issue of consent, which is central to identifying online violence against women as opposed to one's exercise of freedom of expression.

ONLINE VIOLENCE AGAINST WOMEN

What constitutes violence against women has been defined in several international instruments including international and regional declarations, treaties, guidelines and recommendations. In line with the 1993 UN Declaration on the Elimination of Violence against Women, this paper defines "violence against women" as an act of gender-based violence (GBV) that results in, or is likely to result in, physical, sexual, psychological or economic harm or suffering to women, including threats of such acts, coercion or arbitrary deprivation of liberty, whether occurring in public or in private life.[9]

9 Violence against women has been defined and elaborated in many human rights and feminist instruments and discourse including the Convention on the Elimination of all Forms of Discrimination Against Women (CEDAW). The following forms of violence share similarities to online violence against women: intimate partner violence, domestic violence, sexual harassment, harassment based on gender, stalking and inciting others to commit violence against women.

While the perpetration of online violence against women is somewhat new, which itself poses its own challenges, it shares its basis with other forms of violence against women. Although some forms of online violence against women require and deserve further exploration, at this juncture the paper will not attempt to exhaustively define online violence against women.

Suffice it to say that online violence against women consists of acts of gender-based violence that are committed, abetted or aggravated, in part or fully, by the use of information and communication technologies (ICTs)[10] and include, amongst others, cyberstalking, bullying, threats, blackmail and sexual harassment; accessing or uploading/disseminating intimate photos, videos or audio clips without consent; accessing or disseminating private data without consent; uploading/disseminating altered photos or videos through dating, pornography or other kinds of websites; creating fake profiles and other forms of identity theft; mob attacks;[11] grooming predation (of children in particular); doxxing (searching and publicising another's personal data) and exploitation of women and girls.

Online violence against women presents specific challenges. What is actionable and what is not, is crucial in gauging which data or images constitute violence. Actionable violence (including threats of violence) is gauged by intent to harm, content, credibility or imminence of harm and context.[12] In this paper, data and images that constitute actionable online violence against women are deemed violating material.

Where online violence against women does not involve physical violence, it tends to be trivialised, and thus receive inadequate and inappropriate responses from concerned actors, including the state, the private sector, civil society, and society at large, even women themselves. It is thus crucial to look at the responses of different actors, particularly, the identification and role of first responders (including the police, internet intermediaries and helplines), regulators and the judiciary to map the reality of women's initial experiences when accessing justice/remedies, as this colours the rest of the reporting process.

To some extent, these challenges are shared with other forms of violence against women which do not involve physical harm, such as conventional stalking and sexual harassment. Similar to online violence, harassment and stalking often involve repeated acts. While an individual incident could be lawful expression, repeated unwanted acts constitute unlawful harassment or stalking. It is worth noting that because of the ease with which things can be shared, liked, reposted, stored and downloaded, there is more scope for repetition and dissemination of content constituting online violence.

Perpetrators of online violence against women often employ a continuum of violence against women, both offline and online. Like other forms of violence against women, perpetrators are often known to the survivors and include intimate partners and ex-partners.[13]

As with physical stalking, non-physical stalking can evolve into extreme physical violence. Stalking began receiving recognition after model-actress Rebecca Shaeffer was murdered in 1989 by an obsessed fan who had been stalking her.[14] Since the Shaeffer case, stalking, including cyber stalking, has received somewhat more attention and legal response.[15]

Another alarming form of online violence is live streaming of offline acts of violence. While cyber stalking and online sexual harassment do not involve physical violence, in these instances, crimes, including gang rape, are committed in a physical offline space and streamed

10 Association for Progressive Communications (APC). (2015). *From Impunity to Justice: Domestic legal remedies for cases of technology-related violence against women*. www.genderit.org/sites/default/upload/flow_domestic_legal_remedies.pdf

11 For example, the online attack on Leslie Jones on Twitter and the hacking of her iCloud and cell phone. Twitter later suspended one of the attackers. See: www.nytimes.com/2016/07/20/movies/leslie-jones-star-of-ghostbusters-becomes-a-target-of-online-trolls.html and www.ibtimes.com/leslie-jones-hacked-timeline-ghostbusters-stars-twitter-hate-online-attackers-2407046

12 See Delfi AS v Estonia (Application no. 64569/09), European Court of Human Rights, 16 June 2015 for discussion on what constitutes actionable acts.

13 APC research indicates that in approximately 40% of cases of online violence, the perpetrator is known to the victim/survivor.

14 Associated Press. (2014, 14 July). The celebrity murder that changed how stalkers are treated. *Page Six*. pagesix.com/2014/07/14/stars-safer-since-actress-1989-murder

15 Subsequently, California enacted laws criminalising stalking. Criminal stalking is defined in California as "someone who willfully, maliciously and repeatedly follows or harasses another victim and who makes a credible threat with the intent to place the victim or victim's immediate family in fear of their safety." Continuity of purpose must be established through more than one incident. However, where stalking itself is not a crime, for example, in the UK, "offenders get shorter prison sentences that won't make any difference and they go back to stalking." In the UK, a national stalking clinic was opened in London. See: www.dailymail.co.uk/news/article-2071219/Worlds-clinic-treat-STALKERS-prevent-violent-crime-opens.html#ixzz3fSnXU858

live by perpetrators.[16] With social media, crime and self-promotion are intertwined, resulting in a macabre "crime performance" where perpetrators share pre-crime plans, live streaming of themselves in the act of committing the crime and post-crime bragging. "The social media dynamic that drives offenders to post their crime performances has also influenced the treatment of crime victims, so that 'performance victimisation' is also a new reality."[17]

Online violence shares similarities with other forms of crimes, quasi-crimes and torts such as defamation, extortion (blackmail) and non-consensual disclosure of private data, communications and images; hate speech; and child pornography. Incitement to harm is another possible actionable violation. Incitement comprises both incitement against a group and incitement against an individual. Harm comprises both physical and psychological harm.

Thus, sending threatening or offensive material, sharing a persons' private data online and bombarding someone with sexually demeaning emails all constitute violence against women. Furthermore, similar to offline sexual harassment, online harassment or bullying can constitute gross misconduct and grounds for dismissal of an employee, particularly if the employer already has policies on what conduct will be deemed unacceptable irrespective of whether such conduct occurs at the workplace or otherwise. In the Irish case of *Teggart v TeleTech UK Limited,* the court affirmed the dismissal of an employee, finding, amongst others, that the cumulative impact of the obscene Facebook posts about a co-worker, the intention to create a humiliating work environment and the dissemination of the comments among fellow employees justified the dismissal as having been reasonable.[18]

16 Reuters. (2017, 23 January). Three men arrested in Sweden after Facebook Live 'gang-rape'. *The Guardian.* https://www.theguardian.com/world/2017/jan/23/three-men-arrested-sweden-facebook-live-gang-rape-uppsala; Solon, O. (2017, 27 January). Why rising numbers of criminals are using Facebook Live to film their acts. *The Guardian.* https://www.theguardian.com/technology/2017/jan/27/rising-numbers-of-criminals-are-using-facebook-to-document-their-crimes

17 Surette, R. (2015). Performance Crime and Justice. *Current Issues in Criminal Justice*. www.austlii.edu.au/au/journals/CICrimJust/2015/21.html

18 Teggart v TeleTech UK Limited [2012] NIIT 00704_11IT (15 March 2012).

Consent

Consent is key in differentiating lawful from unlawful and harmful behaviour. Consent in relation to online violence is often complicated by the exact act to which the consent, if any, relates. Because of this, defining consent is crucial in online violence and must be addressed in any mechanism dealing with it.

Consent is particularly important in gauging whether there has been violation of privacy with regard to dissemination of private data. Consent that is specific to an individual, like sharing of intimate photos, cannot be expanded to consent for the data to be shared and disseminated more widely.

Focusing on consent also recognises that women have the right to sexual expression, in other words that there is nothing intrinsically unlawful or immoral about expressing oneself sexually through digital images. It is not the taking, but the spreading of these images, videos or other private data that is unlawful or immoral.

Furthermore, in the digitised world of big data, what is personal and what is public data is blurred. Our personal data is continuously being handled and commoditised by internet corporations.[19] It is stored in servers that are liable to be hacked. Such personal data, however, is no less personal even though it may be available in the public domain. This further emphasises that consent for its dissemination is crucial in determining whether a violation of privacy has been committed.

Stigmatisation of victims

Patriarchy and prevailing interpretations of moral norms, culture and religion situate women as the primary bearers of honour and tradition. Transgressions or deemed transgressions of culture by women are viewed as more reprehensible and dealt with by society more severely than those committed by men. This renders women more vulnerable and susceptible to "moral" and "cultural" attacks, particularly sexually nuanced attacks; and less likely to report gender-based violence.

19 Personal data means any information relating to an identified or identifiable individual; an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification number (e.g. social security number) or one or more factors specific to his or her physical, physiological, mental, economic, cultural or social identity (e.g. name and first name, date of birth, biometrics data, fingerprints and DNA).

Victims/survivors themselves may believe that they transgressed social and cultural norms and are to be blamed for the violence committed against them. Women who establish cyber-friendships or relationships may be deemed to have transgressed culturally appropriate behaviour, as are women who engage in sexting or those who consent to intimate partners taking suggestive images, albeit for private purposes. While the relative anonymity available online allows women to transgress and challenge cultural norms, especially in relation to sexuality, the same anonymity combined with the speed, ease and reach of transmission provides a conducive environment for extortion. If the violence involves the uploading of suggestive or sexually explicit images and conversations either maliciously or without the victim's/survivor's consent, then the victim/survivor herself, more than the perpetrator, tends to bear the brunt of societal condemnation.

As a consequence, victims/survivors may be reluctant to seek assistance, silenced and isolated by shame. State actors' decisions to prosecute may be imbued with biases, and susceptible to negative socio-cultural perceptions that imply that victims/survivors provoked the violence through misbehaviour or transgression of socio-cultural norms.[20] This ultimately translates to a lack of support for the victims/survivors of online violence against women. As the internet and digital technology become increasingly integrated in our lives, robust policies are required to curb exposure to online violence.[21]

Outreach programmes can end isolation and remove stigma. The availability of a social network also increases women's autonomy and their ability to seek support and assistance. However, women's access to justice lies both within and beyond legal measures and within the interplay of politics, economics and culture, thus both legal and extralegal (e.g. cultural) remedies are needed.

Ease of transmission and persistence

ICTs amplify the transmission of digital material. ICTs allow for the *easy and rapid dissemination* of information and content, provide multiple platforms, and are comprised of vast networks.

Further, violent content, once disclosed or disseminated, is difficult to remove from these networks. It becomes persistent and remains accessible. The nature of the internet facilitates the transmission of the offending messages and images by others. This problem is made worse by the attitude of internet intermediaries. Platform providers have consistently denied requests from victims/survivors to remove harmful content, irrespective of whether the upload and dissemination of the content was done with the victim's/survivor's consent, whether the images were spliced or otherwise altered to appear as that of the victim/survivor or whether sexually explicit or suggestive content was falsely made to appear to originate from the victim/survivor.

This aggravates the harm to the exercise and enjoyment of human rights and freedoms, particularly the right to privacy or respect for private life caused by the communication of the violating material compared to other forms of more traditional media.[22]

ACTORS AND STAKEHOLDERS

This part discusses three actors and stakeholders involved in online violence. Firstly, the person initiating the violence, namely the author, or the person who first uploads the offending data or images. This is the primary perpetrator. Secondly, the person who purposefully, recklessly or negligently downloads, forwards, or shares the offending data or images. Lastly, the internet intermediaries on whose platforms online violence is perpetrated.

PRIMARY PERPETRATOR

As stated above, ICTs amplify both the anonymity and reach of transmission. The individual who generates the offending data or image is clearly the primary perpetrator. However, legal enforcement officers often lack the training, skill or resources to identify perpetrators who employ protocols to shield their identity, thus offering little or no protection for victims/survivors.

The enhanced anonymity offered by digital and virtual spaces, through encryption and privacy protocols, provides particular challenges in identifying perpetrators of violence against women, including those who engage in harassment, stalking, incitement to harm and defamation. In turn, this magnifies impunity.

20 Abdul Aziz, Z., & Moussa, J. (2013). Op. cit.

21 Ibid.

22 European Court of Human Rights, Editorial Board of Pravoye Delo and Shtekel v. Ukraine, § 63 (Application no. 33014/05), 5 May 2011.

The inability of law enforcement and intelligence services to uncloak anonymity or decipher encrypted communications to investigate crimes has raised "legitimate concerns about how bullies and criminals use new technologies to facilitate harassment."[23] Over-regulation, on the other hand, can lead to online censorship, mass and targeted surveillance and data collection, digital attacks on civil society and repression. Restrictions to encryption and anonymity tools put the privacy of all internet users at risk.[24]

The internet thus offers unprecedented capacity for criminals, pranksters, governments and corporations to interfere with the rights to freedom of opinion and expression. To some extent, encryption, anonymity and the concept of security behind them are essential in the face of political censorship, as they create a zone of privacy to protect opinion and belief.[25] The internet, having become a "central global public forum", deserves protection. Further, "such security may be essential for the exercise of other rights, including economic rights, privacy, due process, freedom of peaceful assembly and association, and the right to life and bodily integrity."[26]

The anonymity provided by these protocols is beneficial to whistle-blowers and human rights defenders, those who oppose current dominant groups or those who are under historical social/cultural/political surveillance because of their identity including black/indigenous/migrant/women, sex workers, young women and those identifying as LGBTIQ. Anonymity also offers privacy for victims/survivors (whose privacy is often violated by perpetrators) and allows them to re-enter online spaces (under pseudonyms, for example). It is simplistic therefore to view anonymity as a threat that needs to be removed under all circumstances.

It is thus critical to formulate principles and guidelines that allow the internet to continue to be the central global public forum that defends the right to privacy and is free from government censorship on the one hand, yet ensure that it is not used as an instrument to commit violations of women's human rights. With warrants and technical skills, the perpetrators can sometimes be identified, especially if the perpetrator is known to the victim/survivor, which allows investigators to trace links to the perpetrator.

23 Kaye, D. (2015). Report of the Special Rapporteur to the Human Rights Council on the use of encryption and anonymity to exercise the rights to freedom of opinion and expression in the digital age. www.ohchr.org/EN/HRBodies/HRC/RegularSessions/Session29/Documents/A.HRC.29.32_AEV.doc

24 Ibid.

25 Ibid.

26 Ibid.

SECONDARY PERPETRATORS

Given the ease and speed of transmission, eliminating online violence against women includes not only addressing and eliminating the primary violation (by the principal perpetrator) but also the dissemination, whether witting or unwitting, by others (secondary perpetrators). Once posted, the offensive material may generally be accessed by others who may download the material and share it by reposting or by creating a link to the material. These others may then take action to discriminate or commit hostile or violent acts against the victim/survivor, for example, by directly communicating with the victim/survivor or related persons.

Even when primary perpetrators are held liable, little attention and effort are directed to holding these secondary perpetrators liable. Data and images that are tweeted and re-tweeted, downloaded and forwarded, liked and shared may involve a great number of individuals and pose an overwhelming challenge to regulators. Further reflection is needed on how to hold re-transmitters responsible for the transmission of violating materials.

Intent, or more specifically, lack of intent, can be an issue with secondary perpetrators. Still, holding persons accountable despite lack of intent is not without basis under the law. In many jurisdictions, criminal law has developed the concept of reckless indifference where intent cannot be established. For example, a person who drives his vehicle into a restaurant is liable for the injuries and deaths caused thereby, even though he may not have intended to injure or cause death, as he is recklessly indifferent as to whether there are persons who would be injured or killed by his actions.

In the civil (non-criminal) realm, negligence is an established element of some tortious act that does not require intent to be established. Another example is the established liability of persons repeating slanderous or defamatory statements. Generally, a person who repeats slanderous or defamatory information is also liable. Under certain circumstances, this liability is irrespective of whether that person is aware that the statement is defamatory, as dissemination does not render an act less offensive or less harmful.[27]

If online violence against women follows these paradigms, secondary perpetrators can be made liable for their action in re-transmitting the offending data or images. At the very

27 "A false statement is not less libelous because it is the repetition of rumor or gossip or of statements or allegations that others have made concerning the matter." Ray v. Citizen-News Co. (1936) 14 Cal.App.2d 6, 8-9.

least, they can be seen as aiders or abettors of a wrongful act although they may not personally know the perpetrator or victim/survivor. After all, ignorance of the identity of the victim/survivor does not make the violence victimless or the harm unforeseeable. It is reasonable to expect that, at the very least, the protection afforded to victims/survivors of offline violence should be made available for online violence.

Internet intermediaries

The internet plays an important role in enhancing access to and facilitating the dissemination of information. It is important that freedom of expression and freedom of information are protected online.[28] Internet intermediaries bring together or facilitate transactions between third parties on the internet. They give access to, host, transmit and index content, products and services originated by third parties. This can take place on the internet or by providing internet-based services to third parties.[29]

Because of the internet's capacity to store and communicate staggering amounts of information, internet intermediaries are placed in a unique position.[30] Many policy and law makers regard protecting internet intermediaries from liability as a prerequisite to protecting the digital economy to encourage the innovation and creativity that have led to the rapid and successful development of the internet. However, others try to enforce barriers to expression and innovation through disproportionate or heavy-handed liability such as unduly requiring intermediaries to monitor content and data being hosted or transmitted online. This hinders the right to freedom of expression as recognised at the international level.[31]

Internet intermediaries are not monolithic. While some merely host or transmit data, like cloud services or small hosting companies, others are increasingly taking on an "active role" mediating content. This can be by performing different and competing roles simultaneously, providing both hosting services and other categories of services. Shielding internet intermediaries from liability is more straightforward when their roles are limited to merely transmitting, hosting and conveying third party information; their defence being generally referred to as "hosting defence". These expanded roles, however, challenge the very bases of the "hosting defence".[32]

Violating materials may not be posted by internet intermediaries nor do these corporations have possession of private data and images which are disclosed and disseminated. Nevertheless, the intermediaries have a responsibility to put in place preventive measures and respond to violating materials, especially when they have the capacity to moderate content and have in place measures to flag and report "user-generated" content.[33]

Thus, free speech as we understand it and as mediated by these corporations is increasingly becoming nebulous and dependent on the "protective" measures put in place by the intermediaries themselves. As online violence happens not merely on the first upload by the primary perpetrator, but is repeated every time it is liked and shared, re-tweeted, searched and downloaded or forwarded, internet intermediaries are uniquely situated to stop the recurrence of the violence and provide the necessary relief and remedy needed by victims/survivors.

Freedom of expression requires the free flow and exchange of ideas and knowledge; but for profit-driven internet intermediary corporations, maintaining the free flow and exchange of ideas and knowledge may be more profitable than eliminating violence against women. Profit plays a significant role in deciding where intermediaries lean when tensions arise between the right of women to a safe internet environment and the interest of internet intermediaries to guarantee their users' freedom of expression and access to information. There are precedents where the courts have been "mindful of the risk of harm posed by content and communications on the internet" and demanded greater vigilance from internet intermediaries.[34]

28 See Human Rights Council resolutions 20/8 (ap.ohchr.org/documents/dpage_e.aspx?si=A/HRC/RES/20/8), 26/13 (ap.ohchr.org/documents/dpage_e.aspx?si=A/HRC/RES/26/13) and 32/13 (ap.ohchr.org/documents/dpage_e.aspx?si=A/HRC/RES/32/13) on "The promotion, protection and enjoyment of human rights on the Internet", which affirm that the same rights that people have offline must also be protected online.

29 OECD. (2010). *The Economic and Social Role of Internet Intermediaries*. www.oecd.org/internet/ieconomy/44949023.pdf

30 European Court of Human Rights, Ahmet Yıldırım v Turkey, § 48 (Application no.3111/10), 2012, and Times Newspapers Ltd, § 27.

31 Electronic Frontier Foundation. (2015). *The Manila Principles on Intermediary Liability Background Paper.* https://www.eff.org/files/2015/07/08/manila_principles_background_paper.pdf

32 For an elaboration of the "active role" standard used, see OECD. (2010). Op. cit.

33 Compare this to the more traditional media such as newspapers. Statements carried in newspapers are vetted and edited, as necessary. Thus the level of control over newspapers is much higher than the control exerted by internet and digital platform providers.

34 See Delfi AS v Estonia (Application no. 64569/09), European Court of Human Rights, 16 June 2015. Although Delfi did not involve violence against women, this dictum is persuasive and is applicable to online violence. See also Yıldırım, A., cited above, and Times Newspapers Ltd, cited above. The Court reiterates that it is also mindful of the risk of harm posed by content and communications on the internet (see Editorial Board of Pravoye Delo and Shtekel, cited above).

It is also more cost effective to seek redress from internet intermediaries than all the re-transmitters (which in fact may not even be logistically possible). For these reasons, intermediaries are best placed to bring online violence activities to an end and their proactive response and co-operation is necessary to eliminate online violence against women.

APPLICATION OF INTERNATIONAL LAW

This part looks at international law and issues of accountability. It explores state responsibility to eliminate online violence which includes states exercising due diligence to prevent online violence, protect victims/survivors, prosecute perpetrators and provide redress and reparation for victims/survivors.

Separately, this part also explores the obligations and duties of internet intermediaries in international law (as opposed to domestic/national laws formulated by states to regulate intermediaries). It looks at the evolution of investing human rights responsibilities and obligations on transnational companies and suggests how these can be complied with.

HUMAN RIGHTS AND THE STATE

Human rights are universal, inalienable, interrelated, interdependent and indivisible. International human rights law protects the right to dignity and equality, prohibiting gender-based discrimination and gender-based violence.[35] International law also protects freedom of expression.

The exercise of these rights under international human rights law is not absolute and may be subject to certain restrictions, but these shall only be such as are provided by law and are necessary for the respect of the rights or reputations of others, or for the protection of national security, public order, public health or morals, and are proportionate to the aim they seek to address.[36]

The application of these restrictions by states, however, "may not put in jeopardy the right itself."[37]

Thus an individual's human rights are not absolute in that they cannot be enjoyed at the expense of the human rights of others. "Others", in this instance, relates to other persons individually or as members of a community:

> Freedom of speech, especially when it concerns expression on the internet, is the absolute foundation of our societal discourse, nonetheless freedom of speech naturally ends where threats abound. It is not freedom of expression to consciously intimidate people on Facebook and Twitter, especially women, insult them, express the wish to rape them or to threaten physical harm. One has to act on this even across borders.[38]

This is different from freedom of opinion. The right to hold opinions without interference is an absolute right and "permits no exception or restriction."[39] However, the expression of an opinion, that is, the right to freedom of expression bears "special duties and responsibilities."

The Sustainable Development Goals recognise that "gender equality is not only a fundamental human right, but a necessary foundation for a peaceful, prosperous and sustainable world. Providing women and girls with equal access to education, health care, decent work, and representation in political and economic decision-making processes will fuel sustainable economies and benefit societies and humanity at large."[40] Violence against women, offline and online, must be acknowledged as a manifestation of the systemic marginalisation of women throughout society. Enhancing "the use of enabling technology, in particular information and communications technology, to promote the empowerment of women"[41] requires the elimination of online violence against women.

35 UN General Assembly. (1948). Universal Declaration of Human Rights. www.refworld.org/docid/3ae6b3712c.html; UN General Assembly. (1979). Convention on the Elimination of All Forms of Discrimination against Women. www.refworld.org/docid/3ae6b3970.html

36 International Covenant on Civil and Political Rights (ICCPR), Article 3.

37 UN Doc. CCPR/C/GC/34, Human Rights Committee, General Comment 34 on Article 19 of the ICCPR, Freedoms of opinion and expression, adopted at the 102nd session, 12/9/11, para 21.

38 Reintke, T. (2016). *Report on gender equality and empowering women in the digital age*. European Parliament, AB-80048/2016. www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//NONSGML+REPORT+A8-2016-0048+0+DOC+PDF+V0//EN

39 UN Doc. CCPR/C/GC/34, Human Rights Committee, General Comment 34 on Article 19 of the ICCPR, Freedoms of opinion and expression, adopted at the 102nd session, 12/9/11, para. 9.

40 www.un.org/sustainabledevelopment/sustainable-development-goals

41 Sustainable Development Goals, Goal 5 target. www.un.org/sustainabledevelopment/gender-equality

Article 20 of the International Covenant on Civil and Political Rights prohibits any advocacy of national, racial or religious hatred that constitutes incitement to discrimination, hostility or violence.[42] Advocacy of gender-based hatred that constitutes incitement to discrimination, hostility or violence should similarly be regarded as a violation of human rights. Effective measures to limit the dissemination of hate speech and speech inciting discrimination, hostility or violence can by no means be equated to "private censorship".[43] Although the Rabat Plan of Action prohibits advocacy of national, racial or religious hatred (and not gender-based hate speech), it is still useful at this juncture to refer to the three types of expression mentioned in the Plan as constituting hate speech, namely expression: (i) that constitutes a criminal offence; (ii) that is not criminally punishable but may justify a civil suit or administrative sanctions; (iii) that does not give rise to criminal, civil or administrative sanctions but still raises a concern in terms of tolerance, civility and respect for the rights of others.[44]

The European Union has also entered into agreements with prominent internet intermediaries, such as Facebook, Twitter and YouTube, to prevent the spread of illegal hate speech online, to educate and raise awareness with their users about illegal hate speech, to develop internal "procedures and staff training to guarantee that they review the majority of valid notifications for removal of illegal hate speech in less than 24 hours and remove or disable access to such content, if necessary."[45] Internet intermediaries also announced that they would "continue to work with the EU to identify and discredit extremist speech by promoting so-called 'counter-narratives' and supporting educational programs that encourage critical thinking."[46] The focus of this initiative, however, is racism, xenophobia and the radicalisation of young people and racist use of platforms to spread violence and hatred.[47] This "code of conduct" was, however, heavily criticised for undermining legal speech, circumventing the rule of law and for the absence of independent oversight.[48]

Several domestic laws similarly prohibit a narrow class of hate crimes, namely on the basis of race, religion, or national origin, but not gender, gender identity, sexual orientation or disability.[49] Further, there are some states that recognise hate speech on the basis of gender or sex, e.g. Canada, Croatia, the Netherlands and South Africa. In order for international and regional initiatives on hate speech to apply to gender-based online violence against women, gender must be included as a category of hate speech that is illegal.

Hate speech, however, must be narrowly defined. For hate speech to be criminalised, it must be of a public nature, at the very minimum present a real and imminent danger, and contain the obvious intention to harm.[50]

Lastly, privacy is another protected human right entrenched in, among others, the Universal Declaration of Human Rights.[51] Invasion of privacy can be established when an individual, in possession of private information, makes a public disclosure of such information without consent.[52]

42 UN General Assembly. (1966, 16 December). *International Covenant on Civil and Political Rights.* United Nations, Treaty Series, vol. 999, p. 171. www.refworld.org/docid/3ae6b3aa0.html and www.ohchr.org/en/professionalinterest/pages/ccpr.aspx. See also Rabat Plan of Action on the prohibition of advocacy of national, racial or religious hatred that constitutes incitement to discrimination, hostility or violence which similarly only prohibits advocacy of national, racial or religious hatred that constitutes incitement to discrimination, hostility or violence. Gender-based hatred should be similarly prohibited. www.ohchr.org/Documents/Issues/Opinion/SeminarRabat/Rabat_draft_outcome.pdf

43 Ibid.

44 Rabat Plan of Action on the prohibition of advocacy of national, racial or religious hatred that constitutes incitement to discrimination, hostility or violence. www.ohchr.org/Documents/Issues/Opinion/SeminarRabat/Rabat_draft_outcome.pdf

45 European Commission. (2016, 31 May). European Commission and IT Companies announce Code of Conduct on illegal online hate speech. europa.eu/rapid/press-release_IP-16-1937_en.htm

46 Drozdiak, N. (2016, 31 May). U.S. Tech Firms Agree to EU Code of Conduct on Terror and Hate Content. *Wall Street Journal.* www.wsj.com/articles/u-s-tech-companies-sign-up-to-eu-code-of-conduct-on-terror-1464689959

47 Ibid.

48 Access Now (2016, 31 May). EDRi and Access Now withdraw from the EU Commission IT Forum discussions. https://edri.org/edri-access-now-withdraw-eu-commission-forum-discussions/

49 This was the case in the US until the passing of the Matthew Shepard and James Byrd, Jr Act.

50 La Rue, F. (2012, 7 September). Report of the Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression (A/67/357). https://www.un.org/en/ga/search/view_doc.asp?symbol=A/67/357

51 Article 12 states, "No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon his honour and reputation. Everyone has the right to the protection of the law against such interference or attacks."

52 In some cases, for the action to succeed, the public disclosure of the facts in question must be highly offensive to a reasonable person of ordinary sensibilities. In other cases, such a test is not applicable, for example, where the data consist of a person's phone number, address or bank account details.

HUMAN RIGHTS AND INTERNET INTERMEDIARIES

State obligation to ensure compliance by business enterprises

Eliminating online violence requires the intercession of internet intermediaries, including transnational corporations serving the role of internet intermediaries. In 2005, the United Nations Secretary General appointed John Ruggie as his Special Representative on the Issue of Human Rights and Transnational Corporations and Other Business Enterprises. In 2011, Ruggie released a set of Guiding Principles on Business and Human Rights on Implementing the United Nations "Protect, Respect and Remedy" Framework. The principles provide that "Business enterprises should respect human rights. This means that they should avoid infringing on the human rights of others and should address adverse human rights impacts with which they are involved."

Ruggie called on states to set out clearly the expectation that all business enterprises domiciled in their territory and/or jurisdiction respect human rights throughout their operations:

> There are strong policy reasons for home States to set out clearly the expectation that businesses respect human rights abroad, especially where the State itself is involved in or supports those businesses. The reasons include ensuring predictability for business enterprises by providing coherent and consistent messages, and preserving the State's own reputation.[53]

To this end, states should "provide effective guidance to business enterprises on how to respect human rights throughout their operations" and encourage or require business enterprises to address their human rights impacts.

Transnational corporations' international human rights responsibilities independently of state obligations

While international human rights law principally focuses on states as subjects of international law, there have been attempts to recognise corporations, especially transnational corporations as having been imbued with international personality and thus recognised as subjects of international law. This has occurred both at the behest of transnational corporations that seek to operate in the international realm and to access international law, as well as at the behest of states that respond by attempting to regulate transnational corporations' activities and imbue them with responsibilities similar to those vested in states.[54]

When can transnational companies be held to be subjects of international law? Courts and international human rights instruments have traditionally been focused on limiting the power of public (state) and not private actors. Courts adjudicating human rights matters generally preclude cases being brought against non-state defendants/respondents. Likewise constitutional guarantees on fundamental liberties and rights are generally enforceable only against the state.

While states have a vested interest in maintaining their power and monopoly in international law by not acknowledging transnational corporations as subjects of international law, transnational corporations wield tremendous influence. Their burgeoning budgets rival the largest of states and they have access to tremendous resources which directly influence, if not directly participate in, the international lawmaking process.[55]

Current realities compel more and more scholars and practitioners alike to consider transnational corporations as having acquired a limited personality in international law.[56] A concomitant of international legal personality is the responsibility to respect human rights that exists over and above compliance with national laws and regulations and independently of states' human rights obligations internationally.

53 Ruggie, J. (2011). *Guiding Principles on Business and Human Rights: Implementing the United Nations "Respect, Protect and Remedy Framework"*. The Guiding Principles were proposed to the United Nations Human Rights Council as part of the 2011 report to the Council by then-UN Special Representative on business and human rights John Ruggie.

54 For example, Organisation for Economic Co-operation and Development (OECD) Guidelines, International Labour Organization (ILO) Tripartite Declaration, and UN Global Compact.

55 The International Court, however, adopts a more mundane definition based on the capacity to have rights and obligations under international law and the capacity to bring international claims. See International Court of Justice. (1949). Reparation for Injuries Suffered in the Service of the United Nations, Advisory Opinion, ICJ Reports 1949, p. 174. www.icj-cij.org/en/case/4 This case pertains to the international legal personality of the United Nations.

56 Transnational corporations are increasingly parties to internationalised contracts which specifically state that these contracts are to be governed by international law, thus conferring transnational corporations with specific international capacities, as well as international treaties, particularly those related to investments. See Texaco Calasiatic v. Libyan Arab Republic (Merits), in American Society of International Law. (1978). *International Legal Materials, 17*, 1-37. States too attempt to regulate the behaviour of transnational corporations. See for example the OECD Guidelines for Multinational Enterprises: www.oecd.org/dataoecd/56/36/1922428.pdf

Andrew Clapham summarises the arguments for imbuing non-state actors with human rights obligations to reverse the notion that human rights are the product of the social contract between the state and the individual. This, he argues, allows us to presume that human rights are entitlements enjoyed by everyone and to be respected by everyone – the net result being that states, corporations and individuals all have human rights obligations. The obligations exist irrespective of whether they are enforceable.[57]

Individuals have been held personally liable for a narrow range of international crimes under humanitarian law that are by no means coextensive with the field of human rights.[58] Holding corporations, particularly transnational corporations, accountable has, however, been subjected to more intense debates, although some headway has been made to invest corporations with the responsibility to promote, protect and fulfil human rights.[59]

Transnational corporations' obligations to respect and protect human rights under international law are being developed, with passionate arguments from advocates on both sides. Thus, Part V of this paper demonstrates why it is critical to hold internet intermediaries accountable for taking, or failing to take, reasonable steps to eliminate online violence against women on their platforms and to develop a framework and guiding principles for internet intermediaries' obligation to promote, respect and fulfil human rights in relation to eliminating online violence against women. After all, internet intermediaries can better be held accountable if they are vested with a positive duty to promote, protect and fulfil human rights.

This duty, however, is not equal to the duty borne by states but merely pertains to the violation of human rights occurring on the respective platforms of the intermediaries. Intermediaries, for example, do not have the obligation to prevent violence wherever it may occur, but only violence occurring on their platforms.[60]

This may also better accord with the Ruggie principles of not "infringing on the human rights of others" and "addressing adverse human rights impacts with which they are involved."

ACCOUNTABILITY AND THE DUE DILIGENCE PRINCIPLE

Due diligence principle

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.[61] This further includes the obligation to remove impunity and provide for certainty of punishment of perpetrators of online violence against women.[62] This does not mean that states are per se accountable for acts of non-state actors. All non-state actors are subject to domestic laws and regulations. Non-state actors include transnational and national corporations operating within the jurisdiction of the state.

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.

This principle holds states accountable for violence committed not only by the state or state actors, but also by non-state actors.[63] Though this principle evolved to focus principally on state obligations, the principle is also useful in guiding internet intermediaries in developing and implementing policies to end violence against women on their platforms.

Such measures should be based on data and meaningful consultation with women's human rights advocates and once developed should be made accessible to women victims/survivors and subjected to continual monitoring and evaluation.

57 Clapham, A. (2006). *Human Rights Obligations of Non-State Actors*. Oxford University Press. graduateinstitute.ch/files/live/sites/iheid/files/sites/international_law/shared/international_law/Prof_Clapham_website/docs/HR%20obligations%20of%20non-State%20actors.pdf

58 For example, for war crimes, such as genocide.

59 Ruggie, J. (2011). Op. cit.

60 Comparison can be drawn from imagining a person drowning. Generally, an individual does not owe a duty, even if she or he is an excellent swimmer, to attempt to save a drowning person. However, the pool owner who obtains economic benefit from the use of the pool by others owes a duty to ensure that there are sufficient safeguards to prevent death or drowning in her or his pool.

61 Abdul Aziz, Z., & Moussa, J. (2013). Op. cit.

62 Ibid.

63 Traditionally, states have only been responsible for their own actions or those of their agents. Gradually, public international law developed to mandate states to exercise due diligence to promote, protect and fulfil human rights.

The due diligence principle is further fleshed out by the Due Diligence Project in the areas of prevention, protection, prosecution, punishment and provision of redress (the 5 P's).[64] These P's are interlinked with overlapping issues.

Prevention (P1)

Prevention includes measures to thwart the occurrence of violence against women. Good prevention programmes provide awareness of online violence against women and of information services and legal protection available following the incident. States have the duty to eliminate discrimination against women in accessing ICTs and promote women's participation and enjoyment of the benefits afforded by ICTs. In this respect, states should develop policies and programmes to educate the public about the issues and develop laws to address online violence against women. They should work to develop a counter-narrative to hate speech based on gender. These counter-narratives should not only address hate crimes but also lawful hate speech based on gender.[65]

States and internet intermediaries should deem online violence not merely as another form of violence, but violence that is grounded in discrimination and that prevents women from exercising their freedom of expression and bars their access to technology and internet spaces. Policies and regulations can be developed for internet intermediary corporations to take preventive measures such as including warnings and reminders against online violence against women and against transmitting content that constitutes online violence.

Internet intermediaries too have the responsibility, independently of states, to develop and publicise policies on online violence and adopt reasonable preventive measures to prevent their platforms from being used to perpetrate online violence.

Protection (P2)

Protection focuses on avoiding the recurrence of further violence (which should be immediate if the perpetrator can be identified), the provision of accessible services, and adequate training and sensitisation of first responders.

States and intermediaries need to implement effective measures to stop the recurrence (and often, escalation) of online violence. For online violence, the violence recurs every time violating materials are accessed, downloaded and shared, so protection of victim/survivors requires the proactive action and cooperation of internet intermediaries.[66] Thus, the obligation to protect does not only refer to the treatment of the original material, but the uploading and dissemination of that material which constitutes recurrence of the violence. While the protocol to identify, tag and stop specific files has already been developed and employed in some instances of gender-based violence, particularly those involving children, due consideration should be given to how and when this protocol should be used for other forms of violence against women and girls.[67]

Fear of repercussions by perpetrators is the main reason women give for not seeking redress to stop violence.[68] It is important to note that online violence often accompanies, precedes or escalates into offline violence and protection should therefore include the same protection given to victims/survivors of offline violence, such as the provision of shelters and issuing restraining orders.

Prosecution (P3)

Prosecution refers to the investigation and institution of proceedings against the perpetrators. Where internet intermediaries are concerned, such proceedings may consist of inquiries. While all violence against women is subject to attitudes of marginalisation and victim-blaming, this is more prevalent in cases of online violence, due to the victims' survivors' inability to demonstrate physical harm. Delay is then caused not only by the lower priority accorded to online violence but also by the lack of skills, knowledge and training in investigating online violence. In addition, jurisdictional issues can make it difficult to identify the appropriate law enforcement agency.

All these exacerbate the victims'/survivors' often already low confidence in the police. The Due Diligence Project survey found that civil society organisation respondents often reserved their worst ratings for the police, particularly in deprioritising women's safety and security over other concerns. Negative attitudes lead to underreporting, particularly in societies that have a culture of silence

64 Abdul Aziz, Z., & Moussa, J. (2013). Op. cit.

65 Ostavik, S. (2015). Op. cit.

66 Nyst, C. (2014). *Technology-related violence against women: Recent legislative trends.* Association for Progressive Communications. www.genderit.org/sites/default/upload/flowresearch_cnyst_legtrend_ln.pdf

67 Gallagher, S. (2013, 5 March). Updated: How Verizon found child pornography in its cloud. *Ars Technica.* https://arstechnica.com/information-technology/2013/03/how-verizon-found-a-child-pornographer-in-its-cloud

68 DDP survey's findings.

surrounding violence against women. The excessive time taken to file charges, delays in the investigations, and the number of years that passed before a case was properly considered were all factors that made women victims/survivors desist from "wasting their time" by filing a complaint.

The state is obligated to train legal enforcement officers on online violence and establish affirmative duties to investigate and prosecute; to foster confidence in the police and judiciary; to establish specialised prosecutors and courts; and to develop a multi-sectoral and multi-agency approach.

Punishment (P4)

Punishment refers to the obligation to impose sanctions on perpetrators. The certainty of adequate punishment creates a level of predictability and sends a message that online violence against women will not be tolerated. Punishment should also be capable of preventing recidivism, rehabilitating the perpetrators and deterring others from engaging in violence.

The punishment for online violence is generally lighter than for "physical" offline violence. States should demonstrate a strong political will to eliminate online violence and exercise innovation in formulating appropriate punishment which acknowledges the harm of online violence, not only to the individual victim/survivor but to other women and girls who may be intimidated or influenced by it. This includes the harm of denying women and girls freedom to participate in online spaces as a consequence of online violence against women.

Provision of reparation (P5)

The state is also responsible for providing adequate redress and reparations for victims/survivors. Generally, reparations and restitution to victims of violence include compensation for the costs of quantifiable losses (cost of medical care, loss of wages, and damage to property), injuries and non-quantifiable losses, and for the needs of the victims/survivors of violence to rebuild their lives in the short, medium and long terms, as they transition from a violent situation to a life free from violence. For online violence, remedies must include the rights of victims/survivors to restitution, where possible.

Victims/survivors of violence against women require that such violence be stopped. Due to the repetitive nature of online gender-based violence (violence is repeated every time a person shares, re-tweets, forwards and downloads the violent content), an injunction against the perpetrator alone will not ensure that the violence stops. Delinking searches[69] from and removal (see EU initiative above) of such content are some of the remedies already provided for other forms of illegal content. Decisions to delink or remove violent content, however, must be decided through a transparent process. Such decisions must also be subject to review by relevant independent and impartial judicial tribunals.

STATE AND INTERMEDIARIES' PRACTICES TO ADDRESS ONLINE VIOLENCE

THE STATE

While many states have attempted to address or even criminalise online violence, enforcement has proven seriously problematic due to a lack of mechanisms, procedures and expertise/skills. While some countries have specific laws on online violence against women, others rely on a combination of offences in the existing criminal and civil regimes. Offences within the present legal regime include stalking, sexual harassment, defamation, invasion of privacy, hate speech, breach of intellectual property rights, threats, identity and data theft, and impersonation.

Without specific legislation, some have sought legal workarounds to have images taken down – most commonly the use of copyright law. However, where a victim/survivor opts to access the intellectual property regime, it is not unknown for victims/survivors to be required to prove that the images that were uploaded pertain (belong) to her person by transmitting a naked photo of herself to the authorities. Furthermore, copyright seeks to protect the proprietary interest in an intellectual endeavour such as artwork or written work while in online violence against women, the perpetrator should be held accountable for the violation of the victim's/survivor's human rights, dignity and privacy rather than any

69 European Court of Justice, Google Spain SL and Google Inc. v Agencia Española de Protección de Datos (AEPD) and Mario Costeja González, 13 May 2014. curia.europa.eu/juris/document/document.jsf;jsessionid=9ea7d0f130d541f8e70d076149b29aa5b05819c20f1e.e34KaxiLc3eQc40LaxqMbN4Pa3eRe0?text=&docid=152065&pageIndex=0&doclang=EN&mode=lst&dir=&occ=first&part=1&cid=47107

proprietary interest in the image or conversation as an artwork or written work.

Research findings underline the urgent need for states to address the remedies available to victims/survivors.[70] Like many repetitive forms of violence against women, victims/survivors require cessation of the violence and immediate protection from repercussions either in the form of retribution from the perpetrator or his family/friends or in the form of the victim/survivors being blamed and stigmatised. Yet, online violence poses new challenges in this regard.

Extraterritoriality

States attempting to hold perpetrators, re-transmitters and internet intermediaries accountable are faced with a major complication, namely that some of these individuals and entities may be beyond the reach of a state's jurisdiction. Only in rare cases do states assert territorial jurisdiction over matters occurring outside their physical boundaries. Yet, the global nature of the internet has added an urgent need to re-examine the meaning of extraterritoriality.

In comparative law, a principle exists that even if the act in question originated from outside the physical jurisdiction of the state, the state may assert jurisdiction if the harm arose within the state. For example, if you discharge a gun from one side of a national border, and the bullet crosses the border and kills a person on the other side of the border, which state has jurisdiction? Arguably, the state where the harm occurred has jurisdiction to prosecute the perpetrator, if and when the perpetrator enters the state; or where both states have reciprocal arrangements.

As a result of the global nature of the internet, many courts have commenced asserting jurisdiction even when the intermediary is not located within their jurisdictions. Using this principle, the French courts have, for example, asserted jurisdiction over a California-based company because disputed goods were accessible to the French public, namely, the website "targeted" the relevant public in their jurisdiction.[71]

As the violating material is posted on a third-party platform, often sited beyond the territorial limits of the state concerned, providing remedies and reparation to the victim/survivor has proven to be especially difficult. Takedown notices, removal of links and disclosure of identity can only be undertaken by third parties who may or may not be liable for the violating material having been posted on their platforms. Like any profit-driven entities, intermediaries would prefer to take the path that generates the most traffic and income.

The European Court of Justice bridged the extraterritorial arguments by finding that search engines (and by implication, other corporations) with sales and marketing subsidiaries in the European Union, are subject to European law relating to European Union citizens irrespective of where that data is processed. The Court further ordered Google to delink certain websites in its search engines based in Europe as well as in the US on the grounds that although the English language search engine is based in the US, the search engine can be accessed by individuals in Europe and therefore continually causes harm in Europe.[72]

Assertion of extraterritorial jurisdiction is not without problems. States contest the assertion of extraterritorial jurisdiction by other states in areas as diverse as drugs, taxation, trade sanctions and national security trade controls. Extraterritorial jurisdiction may be deemed as challenging other states' sovereignty and violating international law.[73]

Even where laws are enacted to address online violence against women, weak political infrastructure and the inaction of enforcement officers result in these laws being poorly implemented. Existing domestic laws can be gauged by their ability to address the culture of impunity, and the participation and power of women as active agents in this process. It is imperative that states articulate what constitutes online violence against women (when does an author's ill will or animus toward another become actionable, when does hostility constitute intimidation or threats) and establish training and sensitisation programmes for legal and judicial officers to handle cases of online violence against women competently and effectively.

In other instances, victims/survivors have sought to obtain justice through claims of sexual harassment, invasion of privacy, defamation and misappropriation of name and likeness. Where the criminal or quasi-criminal processes fail to meet women's needs, victims/survivors are normally expected to commence expensive civil actions.

70 Nyst, C. (2014). Op. cit.

71 See Yahoo! v. Association Amicale des déportés d'Auschwitz et des camps de Haute Silésie.

72 Mario Costeja Gonzalez v. Google, decision of the Court of Justice of the European Union in 2014; see Lee, D. (2014, 13 May). What is the 'right to be forgotten'? *BBC*. www.bbc.com/news/technology-27394751

73 For example, unilateral prohibition of exports to unauthorised foreign destinations and US investigation into the North Atlantic Aviation.

Specific laws and policies

Laws on online violence have been passed in several countries including Canada, England, Germany, Israel, New Zealand, South Africa, Wales and several US states. The contents of these laws will briefly be reviewed in this section.

The criminal justice system appears, for the most part, ill equipped and unable to meet the challenges presented by online violence against women. This includes challenges in investigation, prosecution and adjudication of cases involving online violence against women. Even where laws are enacted to address online violence against women, weak political infrastructure and the inaction of enforcement officers result in non-efficacy of these laws; examples of these are the cases in the Democratic Republic of Congo (DRC), Bosnia and Herzegovina, and Colombia.[74]

Still, APC's research indicates that the first responders most approached by women who encounter online violence are the police. Victims/survivors are, however, referred from one agency to another because it is unclear who is responsible or how the complaint should be handled.[75] Furthermore, misogyny and gender insensitivity still exist among those charged with enforcing the law as a result of inadequate training. This results in loss of confidence in the justice systems and discourages women from asserting their rights. It also serves to silence women.

Notable reforms were implemented in California after Shaeffer's death. These include laws that make stalking a crime (felony stalking), availability of long term protection orders (up to ten years) for stalking, restrictions on public access to information from driving records in California, and a specialised Los Angeles police unit that works with prosecutors, attorneys and security details to keep stalkers a safe distance away from their target.[76]

Los Angeles, with its high population of celebrities, appears to have undergone a mindset change, with institutional transformation and policy reform. Changes in police and judicial attitudes to stalking, proactive preventive intervention which includes searching social media and online sites for evidence of stalking, vigilance over the unauthorised release of personal information, including home addresses, investigations that include tracking of digital fingerprints and collaboration with non-state actors all provide a safer environment. Although the impetus for these changes was to protect celebrities, these laws and policies should be made equally applicable to address and eliminate online violence against the general population.

Over the past decade, there have been several prominent incidents of harassment and stalking in South Africa, including the tragic killing of a television journalist, Shadi Rapitso, in 2009. The Protection from Harassment Act came into force on 27 April 2013, enabling individuals subject to online or offline harassment to apply to a competent court for a protection order lasting up to five years. The Act also contains provisions requiring electronic communications service providers to assist courts in identifying perpetrators responsible for harassment; and creates the offence of contravention of protection orders and failure of an electronic communications service provider to furnish required information.[77]

The Cyber-safety Act of Nova Scotia (Canada) came into force in August 2013, enabling individuals subjected to cyber bullying (or, in the case of minors, their parents) to apply to a judicial officer for a protection order against an individual. The legislation came about as a direct result of the death of 17-year-old Nova Scotia student Rehtaeh Parsons, who took her own life after having been subjected to months of harassment and humiliation stemming from the dissemination online of a photo of her being allegedly sexually assaulted. The Act also contains provisions requiring electronic communications service providers to assist courts in identifying individuals responsible for cyber bullying, and creates the tort of cyber bullying, which enables individuals to sue for damages arising out of cyber bullying. [78]

In New Zealand, the Harmful Digital Communications Bill was introduced in the aftermath of the October 2013 "Roast Busters" sex scandal in which a group of Auckland men allegedly lured young girls into group sex and then posted the video of the incidents online. The Act provides victims with a quick and efficient means of redress for harm (defined broadly) caused to individuals by digital communications (including any text message, writing, photograph, picture or recording).[79] The Act also creates an agency to which victims can turn when

74 Nyst, C. (2014). Op. cit.

75 Athar, R. (2015). *From impunity to justice: Improving corporate policies to end technology-related violence against women*. Association for Progressive Communications. www.genderit.org/sites/default/upload/flow_corporate_policies_formatted_final.pdf

76 Associated Press. (2014, 14 July). Op.cit.

77 Nyst, C. (2014). Op. cit.

78 Ibid.

79 The broad definition of harm is somewhat controversial.

they face online abuse; a set of court orders that can be served against Internet hosts and authors upon referral by the aforementioned agency; new civil and criminal offences; and a 48-hour content takedown process whereby individuals can demand that online hosting providers remove content they allege is harmful.[80]

English and Welsh law defines "revenge porn" as "photographs or films which show people engaged in sexual activity or depicted in a sexual way or with their genitals exposed, where what is shown would not usually be seen in public." It covers images shared on and offline without the subject's permission and with the intent to cause harm.[81]

Data protection regulation which exists in some countries may similarly be applied to cases of online violence. Data protection law was held to have applied primarily to outdated and irrelevant data in search results, unless there is a public interest in the data remaining available and even where the search results link to lawfully published content.[82] The European Court of Justice ordered Google search engine to delink the result of searches from specific outdated data.[83] Google in that case was deemed a data controller of personal data.

A case for the right of victims/survivors "to be forgotten" online can be made out by applying data protection regulation on data and images (fake or otherwise) constituting violence against women that were uploaded either maliciously or without consent. Still, there is no absolute right to be forgotten and the "right to be forgotten" is difficult in practice and, if abused, may be in conflict with the right to freedom of expression and access to information.[84] Regulators are divided on whether the Google judgment signals the beginning of a changed approach.[85]

80 Ibid.

81 BBC. (2015, 12 February). 'Revenge porn' illegal under new law in England and Wales. *BBC*. www.bbc.com/news/uk-31429026

82 See the Spanish Data Protection Directive.

83 European Court of Justice, Google Spain SL and Google Inc. v Agencia Española de Protección de Datos (AEPD) and Mario Costeja González, 13 May 2014. The court ordered delinking rather than removal of the data.

84 See Derechos Digitales. (2015, 22 September). What are the implications of the right to be forgotten in the Americas? *IFEX*. https://www.ifex.org/americas/2015/09/22/derecho_olvido

85 Heywood, D. (2014, November). Google Spain and the 'right to be forgotten'. *Global DataHub*. united-kingdom.taylorwessing.com/globaldatahub/article_2014_google_spain.html The European Union has, however, initiated steps to put in place a policy to protect the right of individuals to have their data fully removed when it is no longer needed for the purposes for which it was collected.

Internet intermediaries and platform providers

Whether, when and to what extent platform or service providers should be held liable for third-party content remains unsettled. Mainly the imposition of liability on service providers for third-party content depends on the intermediaries' role. First, did the intermediary provide, for economic purposes, a platform for user-generated comments? Second, did users – whether identified or anonymous – engage in speech which infringes the personal rights of others or amounts to either direct threats of violence or hate speech and incitement to violence against them?

Judicial solutions in civil and common law jurisdictions gradually started allowing claims in authorising infringement; vicarious and contributory liability; inducing infringement; joint wrongdoing (tortfeasorship); aiding and abetting; and negligence. All these developments portend recognition by judges and policy makers that intermediaries should be made "more" responsible.[86]

Intermediaries can serve as the informational and access gateways for infringing activities and are able to prevent or stem the flood of violating materials which are facilitated through the intermediaries' facilities and services. Furthermore, intermediaries are profiting from these activities. Still, intermediaries' responsibility is not one of strict liability and provision must be made for when and how intermediaries' responsibility should be engaged. One example may be that intermediaries should be made responsible after the violating material has been brought to their attention and opportunity given to the intermediary to take the requisite action.[87]

The courts have held, where warranted, that shifting the risk of the victim/survivor obtaining redress to the internet company, which was usually in a better financial position than the perpetrator, was not as such a disproportionate interference with the media company's right to freedom of expression.[88]

86 Seng, D. (2010). *Comparative Analysis of the National Approach to the Liability of Internet Intermediaries*. www.wipo.int/export/sites/www/copyright/en/doc/liability_of_internet_intermediaries.pdf

87 O'Brien, D., & Kayyali, D. (2015, 8 January). Facing the Challenge of Online Harassment. *Electronic Frontier Foundation*. https://www.eff.org/deeplinks/2015/01/facing-challenge-online-harassment

88 Krone Verlags GmbH & Co. KG v. Austria (no. 4), no. 72331/01, § 32, 9 November 2006.

Presently, liability of internet intermediaries largely pertains to copyright infringements. Indeed, potential liability of internet intermediaries for content posted on their platforms "has raised one of the most spirited and fascinating debates in the legal arena, putting right holders, service providers and Internet users at loggerheads."[89]

Copyright interests are represented by huge concerns within a multi-billion dollar industry. Internet intermediaries similarly can have resources and income to rival those of many states. These disputes concern billions of dollars in potential revenue, expenditure and loss. With nearly bottomless financial resources, stakeholders in these disputes are able to engage the best of minds and exert influence over the highest-ranking lawmakers.

The stage set between internet intermediaries and violence against women victims/survivors cannot be further removed from the stage set between copyright concerns and internet intermediaries. Unlike intellectual property protection, which involves big corporations with limitless funds pursuing violators and internet intermediaries and influencing governments, victims/survivors of online violence are everyday women. The high cost of litigation and such formidable opponents as internet intermediaries with resources that rival states can combine to defeat victims/survivors at the outset. These obstacles are especially acute for women who already face greater challenges in accessing justice, such as poor women, female teenagers, younger women and sexual minorities. It also has the effect of bringing more unwanted attention and can prompt recurring instances of the violation, since courts are not always willing to shield the victims/survivors by giving them anonymity.

Internet intermediaries must further establish comprehensive policies on online violence against women. The posting of disclaimers stating that the writers of the comments – and not the applicant company – are accountable for them does not necessarily result in zero liability when violence occurs. Even if legal obligations cannot be proven, advocates are increasingly insisting that social media platforms have an ethical duty to ensure that technology remains accessible to all. This means that online discrimination and violence must end. Firms that refuse to take substantive measures to curb online violence will increasingly become the centre of controversy.

Internet companies are increasingly finding themselves facing a conflict between profits and social justice; and between freedom of expression and the freedom from discrimination. The recent controversy involving Nextdoor, a "private social network for your neighborhood", is an example. In response to accusations of racial profiling by users, Nextdoor initiated simple anti-profiling measures. The site warns users of racial profiling: "Ask yourself – is what I saw actually suspicious, especially if I take race or ethnicity out of the equation?"[90] The concept behind these warnings is what activists have advocated. This is similar to copyright warnings employed by other technology companies before allowing members to upload material.

These companies also release community guidelines emphasising that the posting of comments that are contrary to good practice or contain threats, insults, obscene expressions or vulgarities, or incite hostility, violence or illegal activities, are prohibited. Many portals have an automatic system to delete comments based on stems of certain vulgar words with a notice-and-takedown system in place, whereby anyone could notify the administrator of inappropriate comments by simply clicking on a button designated for that purpose. In addition, on some occasions, administrators have removed inappropriate comments on their own initiative. Both Twitter and Facebook have taken the positive step of opening a dialogue with women's rights groups to receive input into the design of policies and processes.

Still, there has only been one known recent incident of a user having been permanently banned for "participating in or inciting targeted abuse of individuals."[91]

THE WAY FORWARD

THE STATE

Although access to the internet and other digital spaces is most often facilitated by private entities, it is crucial to regard this space not as private but public, albeit

89 Martinet Farano, B. (2012). *Internet Intermediaries' Liability for Copyright and Trademark Infringement: Reconciling the EU and U.S. Approaches*. https://law.stanford.edu/publications/internet-intermediaries-liability-for-copyright-and-trademark-infringement-reconciling-the-eu-and-u-s-approaches

90 Levin, S. (2016, 30 August). What happens when tech firms end up at the center of racism scandals? *The Guardian.* https://www.theguardian.com/technology/2016/aug/30/tech-companies-racial-discrimination-nextdoor-airbnb

91 Milo Yiannopoulos was banned in relation to the online abuse of Leslie Jones. Bates, L. (2016, 21 July). Leslie Jones's Twitter abuse proves relying on users to report bullies isn't enough. *The Guardian.* https://www.theguardian.com/lifeandstyle/womens-blog/2016/jul/21/leslie-joness-twitter-abuse-proves-relying-on-users-to-report-bullies-isnt-enough

controlled by private entities. After all, some of these spaces are accessed by millions of users.

Specific laws on online violence as well as specialised mechanisms with trained and skilled personnel are required to confront and eliminate online violence. However, merely criminalising online violence does not provide the remedy required by online violence victims/survivors. Experience has shown that women's access to justice should be a mix of criminal, civil and administrative processes and include the areas of all the 5 P's, namely in prevention of online violence, protection of victims/survivors, prosecution and punishment of perpetrators and provision of redress and reparation for the victims/survivors.

The state is responsible for establishing regulating mechanisms consisting of an independent authorising entity – though the independent entity should not serve to authorise itself. The regulatory framework must include provision for the possibility of ordering internet and digital intermediaries to divulge information required to identify the perpetrators where circumstances warrant it, through injunctions or injunction-like orders. It must also respect and provide for the right of victims to restitution. This redress should be specific and proportional to the harm, as well as necessary under the circumstances (see the Manila Principles on Intermediary Liability).[92]

Where voluntary self-regulation by intermediaries fails to deliver the remedies needed, states need to establish independent judicial or quasi-judicial mechanisms to assist victims/survivors in obtaining these remedies.

Admittedly, intermediaries are not responsible nor can they be made liable for the initial act of violence, namely that of posting the violating material online. However, the continued accessibility or dissemination of these materials means that the victim/survivor is continually subjected to violence. Under these circumstances, the state must, in compliance with its international obligation of exercising due diligence to eliminate violence against women, hold intermediaries accountable for failure to remedy the harm or allowing their platforms to be the instrument of continued violence after notice of the violence is drawn to their attention.

State regulation must be conscious of not violating freedom of expression yet at the same time, prioritising women's access to online technology in a safe environment where perpetrators of online violence do not enjoy impunity. The state has a positive role in creating an enabling environment for freedom of expression and equality, while recognising that this opens up avenues for potential violence. Strong democratic structures – including free and fair elections, an independent judiciary and a vibrant civil society – are needed to prevent abuse and to realise more fully the goals of pluralism and equitable access.[93] States must also include women's rights organisations in the development of regulations, and adopt a human rights approach.

INTERNET INTERMEDIARIES

Self-regulation by internet intermediaries and platform providers remains the most viable method of imbuing corporations with responsibility. As with offline violence, consent must be the pillar around which both preventive and post-incident policies are formulated. Content that threatens or contains images of rape or sexual and physical violence toward an identified individual or individuals should not be treated as freedom of expression.

Victims/survivors of violence, whether they live on college campuses or in remote villages, require that violence cease; yet postings on the internet have a level of permanence and can repeatedly be searched, accessed and disseminated. Cessation of online violence and the restoration of privacy can only be provided by internet intermediaries and platform providers.

Intermediary corporations must recognise violence against women as unlawful behaviour, and demonstrate increased and expedited cooperation in providing relief to victims/survivors within the corporations' capacities. This could be through systems for cooperating with law enforcement, takedown procedures for abusive and harmful content, and/or the possibility of account termination for misconduct. The intermediaries' reporting procedure and mechanisms, as well as remedies, must be accessible and transparent. Exercising due diligence includes setting out when and how intermediaries are deemed to have had notice of such violence.

Corporations should also create appropriate record keeping systems specific to violence against women, and classify and share the ways in which they have responded

92 https://www.manilaprinciples.org

93 See, for example, ARTICLE 19. (2009). *The Camden Principles on Freedom of Expression and Equality*. https://www.article19.org/data/files/pdfs/standards/the-camden-principles-on-freedom-of-expression-and-equality.pdf

to reports of such violence.[94] Internet intermediaries must also commit to and implement comprehensive human rights standards as well as committing to, and operationalising, the UN Guiding Principles on Business and Human Rights.[95]

The mechanisms set up to respond to violence against women must be available and accessible to victims/survivors regardless of their geographic location. When developing liability rules for intermediaries, it is important that legal requirements are appropriate and proportional to the function and size of the intermediary. Policies must be responsive to all women including those outside Europe and North America. Given that the reach of the internet and digital media is neither limited by nor respectful of geopolitical boundaries, complaint mechanisms should be equally global.

National regulators and regional courts alike have recognised victims'/survivors' rights to restitution, namely their right to have violating materials taken down or de-linked from the result of searches. This right, sometimes referred to, rightly or erroneously, as "the right to be forgotten" compels intermediaries to exercise due diligence under certain circumstances.[96] These circumstances should include materials that constitute violence against women. However, it may be impossible to ensure a complete takedown of the violating material. In such circumstances, certain actions, such as delinking the result of searches to the violating material, may be deemed reasonable and sufficient to stop the harm.[97] These actions must be proportionate and capable of remedying the harm caused.

Intermediaries should also seek to empower users through hotlines, awareness raising and education. More proactive measures such as formulating and publicising anti-violence against women policies and posting reminders and warnings that the content of materials about to be uploaded should not constitute violence against women may go some way toward corporations' meeting their due diligence responsibilities to protect and respect human rights and to provide remedy in case of violations.

However, the ensuing jurisprudence from multiple jurisdictions has resulted in confusing or conflicting court decisions.[98] What is required is an international multi-stakeholder framework that harmonises and prescribes the factors to be considered for indirect internet intermediary liability and the defences available against such liability.[99]

94 This includes the use of multistakeholder policy platforms, such as the Global Network Initiative, as opportunities to share lessons learned and best practices to respond to this issue. www.globalnetworkinitiative.org

95 See also Athar, R. (2015). Op. cit.

96 The "right to be forgotten" is still a debatable concept. Outside the gender-based violence context, the right to be forgotten is sometimes used to compel intermediaries to take down criticisms and political dissent. Alternatively, it is also sought by those who wish to expunge their criminal past. Most recently a Japanese court dismissed the claims of a man convicted of violating child prostitution and pornography laws for his criminal past to be removed from Google search results. "The deletion (of references to the charges from search engines) can be demanded only when value of privacy protection clearly exceeds freedom of expression of search sites," said the Court. McCurry, J. (2017, 1 February). Japanese court rules against paedophile in 'right to be forgotten' online case. *The Guardian*. https://www.theguardian.com/world/2017/feb/02/right-to-be-forgotten-online-suffers-setback-after-japan-court-ruling

97 European Court of Justice, Google Spain SL and Google Inc. v Agencia Española de Protección de Datos (AEPD) and Mario Costeja González, 13 May 2014. curia.europa.eu/juris/document/document.jsf;jsessionid=9ea7d0f130d541f8e70d076149b29aa5b05819c20f1e.e34KaxiLc3eQc40LaxqMbN4Pa3eRe0?text=&docid=152065&pageIndex=0&doclang=EN&mode=lst&dir=&occ=first&part=1&cid=47107. See also Google policy on delinking the content: https://support.google.com/websearch/troubleshooter/3111061#ts=2889054%2C2889099

98 Compare the court decisions of A&M Records Inc v Napster (9th Cir. 2001) and UMG Recordings Inc. et al. v. Veoh Networks Inc et al. (9th Cir. 2011). Napster was held liable for third party infringing content and YouTube not liable despite a high amount of infringing content existing on both platforms.

99 See also the 2016 Report of the Special Rapporteur to the Human Rights Council on Freedom of expression, states and the private sector in the digital age. ap.ohchr.org/documents/dpage_e.aspx?si=A/HRC/32/38

Internet and ICTs for social justice and development

APC is an international network of civil society organisations founded in1990 dedicated to empowering and supporting people working for peace, human rights, development and protection of the environment, through the strategic use of information and communication technologies (ICTs).

We work to build a world in which all people have easy, equal and affordable access to the creative potential of ICTs to improve their lives and create more democratic and egalitarian societies.

www.apc.org info@apc.org

Graphic Design: MONOCROMO

THIS ISSUE PAPER FORMS PART OF THE APC PROJECT "BUILDING FEMINIST CROSS-MOVEMENT COLLABORATION AND ACTION ON INTERNET AND HUMAN RIGHTS IN AFRICA, ASIA AND LATIN AMERICA AND THE CARIBBEAN", FUNDED BY THE FORD FOUNDATION.

DUE DILIGENCE AND ACCOUNTABILITY FOR ONLINE VIOLENCE AGAINST WOMEN
JULY 2017

ISBN 978-92-95102-81-1 APC-201707-WRP-EN-DIGITAL-271