The Due Diligence Project's

Due Diligence to Eliminate Online Violence against Women: The State, Intermediaries and Engendering Universal Access to the Internet

Director: Zarizana Aziz

Submission to the UN Special Rapporteur on Violence against Women, its causes and consequences

February 2018

ACKNOWLEDGEMENTS

The Due Diligence Project would like to acknowledge with gratitude the contributions and collaboration of the following entities whose generous support made the expert meeting on information communication technology related violence against women (ICTV) held on 16 – 17 January 2018 in Washington DC, USA, possible, discussions of which contributed to the preparation of this report:

The Government of Canada

The Association for Progressive Communications

I. INTRODUCTION

The Due Diligence Project[1] (DDP) welcomes the UN Special Rapporteur's thematic focus on violence against women perpetrated partially or fully by the use of information communication technology (ICTV).

The purpose of this contribution is threefold:

- to frame the discussion on highlight new and innovative thinking beyond the current language and discourse in understanding and conceptualizing discrimination and violence against women;
- to critically examine crucial basic concepts which adds to this understanding; and
- to look at technology-based violence against women through the lens of the State Obligation.

The lens of State Obligation is presented through the Due Diligence Framework developed by the Due Diligence Project.[2]

1. Situational Context

Women's and girls ability to access and utilise the transformative potential of the internet is increasingly under threat by high levels of online violence against women and girls (VaW). Increased prevalence of online VaW, 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.

Freedom of expression (FoE) and access to information are fundamental rights and key enablers to a range of human rights. Research in the US indicates that while a gender gap in being online has diminished since 1990, gender gaps in the number of uses of the internet and in the frequency of internet use persists with women having significantly fewer uses of the internet than men. Women also tend to use the internet at work.[3] These figures varies widely between countries and between platforms. In a 2013 survey, the Express Tribune – an English-language Pakistani news daily – measured internet use in Pakistan and found that approximately 70% of users on Facebook were men.[4]

ICTV prevents women and girls from fully exercising their rights. Research in India indicates that 28% of women who had suffered ICTV intentionally reduced their online presence.[5] Removing VaW from digital platforms has the net effect of promoting and strengthening FoE

[1] The Due Diligence Project (DDP) is a global project that explores and unpacks the international legal principle of 'due diligence' in the context of violence against women. www.duediligenceproject.org

[2] Zarizana Abdul Aziz and Janine Moussa, *The Due Diligence Framework: Framework on State Accountability to Eliminate Violence against Women*, International Human Rights Initiative, 2014. The Due Diligence Framework contains guidelines in the five areas of State Obligation, namely prevention, protection, prosecution, punishment and provision of redress and reparation.

[3] Hiroshi Ono and Madeline Zadovny, *Gender and the Internet*, Social Science Quarterly, 84(1)

[4] *Measuring Pakistani Women's Experiences of Online Violence: A Quantitative Research Study on Online Gender-Based Harassment in Pakistan*, Digital Rights Foundation, 2017. Available at http://digitalrightsfoundation.pk/wp-content/uploads/2017/05/Hamara-Internet-Online-Harassment-Report.pdf

[5] Japleen Prasricha, *Violence" Online In India: Cybercrimes Against Women & Minorities on Social Media*, Feminism in India. Available at https://feminisminindia.com/wp-content/uploads/2016/05/FII_cyberbullying_report_website.pdf.

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.[6]

Eliminating ICTV is all the more critical given the increasingly central role of online information and communications technologies. In many instances it has become the main form of communication in commercial dealings as well as personal, political and social interaction.

2. Purpose of submission

In the Due Diligence Project's extensive three year research-advocacy (2010 – 2013) on violence against women, technology-based violence stood out as an understudied issue yet with wide-ranging consequences on women' access to technology. Since 2013 the Due Diligence Project (DDP) has conducted intensive research into online violence, its impact of women and accountability of the State and internet intermediaries and platform providers. While the role of the State as the entity ultimately responsible for preventing and addressing human rights abuses has been a central approach to the work of the Due Diligence Project, in the ICT context, additionally internet intermediaries and platform providers, as well as the technical community have roles to play if violence against women is to be eliminated from these media.

The DDP collaborated with Association for Progressive Communications and convened two expert meetings, the first in November 2015 in Florence, Italy and the second in January 2018 in Washington DC, USA. The meetings engaged with experts on violence against women and freedom of expression from the academia, inter-governmental organisations, civil society to identify critical issues on online violence and explore strategies to eliminate online violence by the State and internet intermediaries within the context of State obligation to promote, protect and fulfill human rights and business enterprise responsibility to protect and respect human rights as well as greater access by victims to effective remedy, both judicial and non-judicial. The participants from the second meeting further included representatives from industry actors (internet intermediaries and platform providers) which provided insight into the many challenges of and initiatives by industry actors to prevent and address ICTV.

Outcomes of the first expert meeting as well as independently conducted research in the area by the DDP are contained in *Due Diligence and Accountability for Technology-based violence against Women (DDP Paper I.)*[7] This submission is offered as a contribution to the discourse on this critical and complex issue and to the UN Special Rapporteur for consideration in her 2018 annual thematic report on violence perpetrated in part or in full through the use of information and communication technology and should be read with the DDP Paper I, which is annexed hereto for easy reference.

3. Concepts and terminology

- **ICT related violence against women:** are acts of gender-based violence against women and girls committed, abetted or aggravated in part or fully by the use of information and communication technologies. This includes but is not limited to cyber stalking, accessing or disseminating a woman's or girl's private data (through hacking), identity theft, doxxing and ICT mob attacks.

[6] Zarizana Abdul Aziz, *Due Diligence and Accountability for Online Violence against Women*. Available at www.duediligenceproject.org and https://www.apc.org/en/pubs/due-diligence-and-accountability-online-violence-against-women.

[7] Zarizana Aziz, *Due Diligence and Accountability for Technology-based violence against Women*. Available at www.duediligenceproject.org and https://www.apc.org/en/pubs/due-diligence-and-accountability-online-violence-against-women.

- **Due diligence:** International law mandates States to exercise due diligence to promote, protect and fulfill human rights. This includes the obligation to prevent violations, protect victims/survivors of human rights abuses, prosecute violations of human rights, 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 includes but is not limited to transnational and national corporations operating within the jurisdiction of the State.[8]

- **Internet intermediaries** bring together or facilitate transactions between third parties on the internet and ICTs. 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. For purposes of this paper, they include internet or digital access providers, internet service providers, network infrastructure providers, platform providers including social platforms.

- **Intermediary obligations** look at the obligations of internet intermediaries within the international framework to respect and protect human rights, not to allow themselves to be complicit in the abuse of these rights by others through or as a consequence of their business operations and to remedy adverse human rights impacts with which they are involved.[9]

- **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.[10] The liability approach in this submission requires intermediaries to act expeditiously to remove content that constitutes actionable ICTV once the intermediaries have notice of the content to ensure that their sites do not serve as vehicles for violating material.[11]

II. Contributions to the Discourse

1. Due Diligence Framework and the Role of the State and Internet Intermediaries

The 'due diligence principle', as it is commonly termed, holds States accountable for human rights abuses committed not only by the State or State actors, but also by non-State actors. Violence against women is perpetrated by both State and non-State actors. By making the

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

9 John Ruggie, *Guiding Principles on Business and Human Rights: Implementing the United Nations "Respect, Protect and Remedy Framework,"* (UN Human Rights Office of the High Commissioner, 2011). 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 & human rights, John Ruggie: *Report of the Special Representative of the Secretary-General on the Issue of Human Rights and Transnational Corporations and Other Business Enterprises, John Ruggie,* UN Doc. A/HRC/17/31, Mar. 21, 2011, *available at* http://www.ohchr.org/Documents/Publications/GuidingPrinciplesBusinessHR_EN.pdf. *See also* Guidelines for Multinational Enterprises of the Organisation for Economic Co-operation and Development and the Ten Principles of the UN Global Compact, available at https://www.unglobalcompact.org/what-is-gc/mission/principles.

10 Intermediary legal liability differs. Some states provide broad protections for intermediaries while others are heavy-handed in requiring intermediaries to monitor content. See discussion in Aziz, DDP Paper I as well as example of the newly passed German legislation below, *supra* n. 42.

11 Reasonableness in removal of content is further discussed below.

State accountable for violence committed by both State and non-State actors, public international law recognizes that violence against women, regardless of who commits it, constitutes human rights violations. The due diligence principle is a critical tool in the formulation of accountability.

The principal importance of the due diligence obligation of the State is its duty to intervene and protect individuals from harm, even where the actors concerned may be private actors (rather than agents of the State).[12] This key principal can be leveraged in developing strategies to protect persons from rights abuses. Due diligence has also ruptured the artificial 'public/private sphere' divide and the dichotomy between State and non-State actors. States are now not only permitted but obliged to ensure that no justification may be invoked for States to deny accountability for discrimination against women.

The Due Diligence Framework is a tool, developed by the Due Diligence Project, to help gauge and assess State compliance with its due diligence obligation effectively to prevent and respond to human rights violations.[13] Derived from international human rights law,[14] the due diligence principle obligates a State to take reasonable action to prevent, protect, punish, and provide redress ("5Ps") for human rights violations. The Framework is organized along the due diligence "5Ps" and supported by Guiding Principles which further break down the 5P's into tangible, actionable, and implementable elements.

The Framework places the role of the State at the centre of the discussion. This is not to say that non-State actors do not, indeed they do, have a role to play in eradication of discrimination against women. But rather the Framework provides a lens for analysis and underscores that the ultimate responsibility and obligation to prevent, address and respond to human rights violations rests with the State.

This emphasis on the role of the State is responsive to the call for a paradigm shift and a more comprehensive and holistic approach to eradication of violence against women. It looks not merely at the programmes policies and laws the State has established, but their effective implementation. That is it requires States to close the implementation gap. The Due Diligence Framework and its Guiding Principles assist in identifying the different actors, stakeholders, and allies; takes into account the socio-economic-historical contexts of women and particular groups of women; and emphasizes the need to address root causes, risk factors and incorporate transformative justice ideals into programmes, laws and policies to eradicate violence against women.

Yet, one fundamental challenge with ICTV is that cyber-space is not within the explicit nor implicit control and jurisdiction of any one State. Eliminating ICT related violence requires the intercession of internet intermediaries, including transnational corporations serving the role of internet intermediaries. Separately, this submission also addresses 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.[15]

[12] See discussion on harm below.
[13] Abdul Aziz and Moussa, *supra* n. 2
[14] See for example, CEDAW General Recommendation no. 19 (1992); Human Rights Council resolutions 11/2 (2009); 14/12 (2010); 20/12 (2012); UN General Assembly resolutions 65/187 (2010), and 69/xx (2014) on State Obligation.
[15] *Supra* n. 7

2. Basic premises and founding principles

➢ *The internet environment*

Like all forms of violence against women, culture plays a critical role in perpetuating ICTV. Internet freedom provides a fertile terrain for an evolving internet culture giving rise to increasing interest in understanding computer-mediated communication. The reduction of non-verbal cues in computer-mediated communication has challenged our social mores learned from face to face interaction.

People may self-disclose or act out more frequently or intensely than they would in person. Researchers have identified six factors that interact with each other in creating this online disinhibition effect: dissociative anonymity, invisibility, asynchronicity, solipsistic introjection, dissociative imagination, and minimization of authority.[16] Consequently, understanding the negative or toxic use of the internet is important.[17]

Understanding these new social mores requires the participation of youths who form the bulk of users adept at computer-mediated communication and gauging their views on security, privacy and regulation, amongst others. It also requires anticipating how social mores will evolve with the next generation of ICT users. Only then can we develop effective strategies to eliminate ICTV from these media.

➢ *Human Rights framework*

Any discussion on ICTV must be framed within the human rights framework, namely universal, inalienable, inter-related, inter-dependent and indivisible. Freedom from gender-based violence against women, freedom of expression and rights to privacy are protected by international human rights law.

Freedom of expression is protected as a public right. Its exercise however, must not impinge on another person's human rights. However, any limitation must be clearly and precisely defined in a substantive and procedural law, it must pursue objectives authorized by human rights and it must be necessary in a democratic society for the attainment of the aims pursued. The limitations must be suitable for accomplishing the intended objective, and strictly proportional to the aims pursued.[18]

ICTV creates an obstacle to women's access and ability to enjoy and exercise this public right. The lack of response, both legal and non-legal, to ICTV and gender discrimination leads to a reduction in women's ability to speak freely, safely and securely. The effect of this phenomenon of exclusion is similar to the effect of censorship: silence.[19]

---

[16] John Suler, *Cyber Psychology & Behavior*, July 2004, 7(3): 321-326

[17] ICT 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. Association for Progressive Communications, *Analysis of Incidents of Technology-related Violence Against Women Reported on the "Take Back the Tech!" Ushahidi Platform* (Sept. 9, 2015). *Available at* http://www.genderit.org/resources/analysis-incidents-reported-take-back-tech-ushahidi-platform. Accessed 1 February 2018.

[18] See for example Art. 13(2) of the *American Convention on Human Rights*, 1969, *Treaty Series, No. 36* 1969. See too Article 19, International Covenant of Civil and Political Right referred to in Aziz, DDP Paper I.

[19] IACHR. Annual Report 2009. Annual Report of the Office of the Special Rapporteur for Freedom of Expression. Chapter III (Inter-American Legal Framework of the Right to Freedom of Expression). OEA/Ser.L/V/II. Doc. 51. December 30, 2009, para. 36

The exercise of freedom of expression is different from freedom of opinion. The right to hold opinions without interference is an absolute right and "permits no exception or restriction".

Effective implementation of strategies policies and laws to eliminating ICTV reinforces freedom of expression by expanding the public space for diverse voices. Eliminating ICTV requires a holistic rather than strictly legal approach. Because freedom of expression is a public right, freedom of expression as a legal right may be enforced differently when expressing oneself at a public forum (for example twitter) and in a private conversation (for example Whats app).

➢ *Actionable ICT VaW*

In this section, three pivotal concepts are discussed. These are harm, aggregated harm and consent (including withdrawal of consent).

The avoidance and prevention of violence constitute the basic purpose of lawmaking. The rule is so fundamental that "if a legal system did not have them there would be no point in having any other rules at all".[20] There is also no society that does not prohibit arbitrary acts of force and habitual and pervasive acts of cruelty.[21]

Like offline non-physical violence, ICTV which does not involve physical violence is often trivialised.[22] For example sextortion, that is extorting sexual favours by blackmail through threats to release sexual information or images. Women who are victims/survivors of sextortion are wont not to report, particularly as they would be stigmatised resulting in sextortion being understudied.[23] The US National Center for Missing and Exploited Children also estimates that about 78% of sextortion victims are girls with an average age of 15.[24] ICT has transformed sexual violence to something that can be perpetrated by perpetrators across physical miles and without physical contact and enli[25]sting anonymous people to amplify the harm to victims/survivors.

Extortion was commonly defined as the acquisition of property or financial gain without the person's consent induced by fear or force. The law appears to only be catching up to new offences facilitated by ICT, such as sextortion. California is one of the few (but increasing) jurisdictions to have passed laws criminalising sextortion. The law expanded the definition from the acquisition of property "anything of value, including enumerated sexual acts or sexual images".[26] The Californian law will go into effect 1st January 2018.

---

[20] Hart, HLA (1958) 'Positivism and the separation of law and morals' *Harvard Law Review* vol 71(4) (February 1958) pp. 593-629.
[21] Weiss and Hubert (2001) *The responsibility to Protect: Research Bibliography, Background : Supplementary Volume to the Report of the International Commission on Intervention and State Sovereignty*, International Development Research Centre, Ottawa, Canada.
[22] For discussion on defining ICTV, refer to Aziz, DDP 1.
[23] Wittes, Benjamin & Ors, *Sextortion: Cybersecurity, teenagers, and remote sexual assault*, Brookings, May 2016. Available at https://www.brookings.edu/wp-content/uploads/2016/05/sextortion1-1.pdf. Accessed 1 February 2018.
[24] Sextortion, *Trends identified in CyberTipline sextortion reports,* National Centre for Missing and Exploited Children. Available at http://www.missingkids.com/theissues/onlineexploitation/sextortion.
[25] Personal data is defined in Aziz, DDP I, n. 19
[26] Senate Bill 500, Chapter 518. Amendments to the Penal Code relation to extortion. Available at https://leginfo.legislature.ca.gov/faces/billTextClient.xhtml?bill_id=201720180SB500 (accessed 12 February 2018)

Another example was highlighted in an Indian research over four years that found that the highest form of ICTV was crank calling women to their mobile phones.[27] In India, 40% of respondents assessing a CSO-operated cyber helpline reported that they were had been harassed or stalked via messaging applications.[28] This form of ICTV has not received much attention, possibly because it is prevalent only in isolated countries. These crank calls were so bad that women are known to have opted not to have mobile phones. Violence also occurs in private conversations on Whatsapp and other chat groups. As with crank calls, these violence, which happen at an individual to individual level, are rarely checked.

Another form of ICTV is the uploading of images of 'beautiful girls" in specific cities and/or disclosure of their personal data (e.g. mobile numbers). In the Indian sub-continent however, women featured in these postings may suffer harm and could be subjected to further violence, both offline and online irrespective or whether these women were voluntary participants.[29]

a) Harm

To understand violence against women, including ICTV, we must look at its personal aspect as committed by a perpetrator and the harm to the victim. VaW is an assault on human dignity. Unlike offline violence, for example, sexual harassment, online or ICTV can be committed at any time from any place. It is essential that we broaden our understanding of VaW to emphasize the harm it causes.

In *United States v. Sayer*[30], the perpetrator stalked his ex-wife online, created fictitious Facebook and Myspace pages in her name, disseminated non-consensual intimate media and made Yahoo messenger profiles to invite men to her home, thereby enlisting third parties to harass his ex-wife. In sentencing the Court considered the fear and danger the perpetrator caused through anonymous third parties, the permanent nature of intimate details posted online and his ongoing obsession with her.

In most instances, ICTV can be gauged by its intent to harm, content, credibility or imminence of harm and context.[31] However, in violations of data, for example the publishing of private or identifying information and images, harm maybe more difficult to establish.

Unless the act is illegal, malicious intent, however, may in appropriate circumstance be sufficient to render an act actionable. This includes acts such as doxxing, where personal information and data retrieved by the perpetrator is made public with malicious intent. For these cases, complainants would need to rely on privacy harms (see below).

b) Aggregated harm

The internet provides a forum where harm can be inflicted in multiples or hundreds or even thousands or millions who had been wittingly or unwittingly enlisted to participate in and re-perpetrate the violence resulting in an aggregate harm. The target may be an individual, such as when a woman's personal details and intimate photos are made public.

In describing the aggregated harm the unauthorized release of her photos cause, the Hollywood actress Jennifer Lawrence said,

---

[27] DDP expert meeting, 16-17 January 2018, Washington DC. Crank calling involves calling someone and hanging up.
[28] *Cyber Harassment One Year Report, December 2017 – November 2018*, Digital Rights Foundation, 2018. Available at https://digitalrightsfoundation.pk/wp-content/uploads/2017/12/Helpline-Annual-Report.pdf
[29] DDP expert meeting, 16-17 January 2018, Washington DC.
[30] *United States v. Sayer*, 748 F.3d 425 (1st Cir. 2014)
[31] Aziz, DDP Paper I

> "When I first found out it was happening, my security reached out to me. It was happening minute-to-minute — it was almost like a ransom situation where they were releasing new ones every hour or so. And, I don't know, I feel like I got gang-banged by the fucking planet — like, there's not one person in the world that is not capable of seeing these intimate photos of me."[32]

Or the target may be women as a class, motivated by gender animus (hate speech based on gender). So far, the recognized restrictions on freedom of expression prohibit any advocacy of national, racial or religious hatred that constitutes incitement to discrimination, hostility or violence. It does not include advocacy of gender hatred.[33] Apart from expressions that constitute crimes or that can be the basis of civil action or administrative sanction, hate speech includes expression that raises a concern in terms of tolerance, civility and respect for the rights of others. [34]

What is needed is a specific restriction on hate speech based on gender or advocacy that constitutes incitement to discrimination, hostility or violence against women. In Mexico, for example, femicide is prevalent. A famous singer had a music video. "Fuiste Mia" ("You were mine"), featuring a man who drags his lover to a car, stuffs her in the trunk and smiles as he sets it on fire. The Mexican Interior Ministry condemned the video, saying, amongst others, it normalized a social scourge.[35] Said Paty de Obeso of the Institute for Economics and Peace in Mexico, "Our challenge is that violence, more than organized, has become cultural. Each time, violence surprises us less and less. It's become part of culture."[36]

Still caution must be exercised in the removal of content that is not illegal. We need to differentiate between what is illegal and what is reprehensible but not illegal. As seen with "Fuiste Mia", the State took action despite the absence of regulation rendering such videos unlawful. While a precedent was established that transformed social acceptance of glorifying femicide to social sanction against gender-based hate expression, vigilance is needed to ensure that these actions do not lead to overreaching and censorship. Overreaching, for example, banning all sexual expression in a bid to eliminate the dissemination of videos glorifying sexual violence, can also harm women by restricting women's own sexual expression or by projecting norms that sexualize all representations of women's bodies, even nursing mothers.

In these situations, the law alone is not enough. What we need is a holistic approach starting from addressing the underlying causes of VaW from a social and cultural perspective.

---

[32] Scott Fienberg, *'Awards Chatter' Podcast — Jennifer Lawrence ('Mother!')* The Hollywood Report, 20 November 2017. Available at https://www.hollywoodreporter.com/race/awards-chatter-podcast-jennifer-lawrence-mother-1059777. Accessed 1 February 2018.

[33] See DDP Paper I. See also *Report of the United Nations High Commissioner for Human Rights on the expert workshops on the prohibition of the incitement to national, racial or religious hatred*, U.N. Doc. A/HRC/22/17/Add.4, Jan. 11, 2013. *Available at* http://www.ohchr.org/Documents/Issues/Opinion/SeminarRabat/Rabat_draft_outcome.pdf (last visited May 23, 2017).

[34] G.A. Res. 2200A (XXI), International Covenant on Civil and Political Rights (Dec. 16, 1966); *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. *See* "Rabat Plan of Action," *available at* http://www.ohchr.org/Documents/Issues/Opinion/SeminarRabat/Rabat_draft_outcome.pdf. Accessed 1 February 2018.

[35] AFP, *Mexican music video showing woman murder sparks outrage*, I 24News, 9 April 2016. Available at https://www.i24news.tv/en/news/international/americas/109095-160409-mexican-music-video-showing-woman-murder-sparks-outrage. Accessed 1 February 2018.

[36] As quoted by Leila Cobo, *Gerardo Ortiz Apologizes for Graphic 'Fuiste Mia' Video, But Should He Be Prosecuted?*, Billboard, 22 July 2016. Available at https://www.billboard.com/articles/columns/latin/7446673/gerardo-ortiz-apologizes-fuiste-mia-video-arrest

c) *Privacy*

Everyone has a legitimate expectation that his or her private life would be protected. This expectation, holds that a person's image "constitutes one of the chief attributes of his or her personality, … The right to the protection of one's image is thus one of the essential components of personal development. It mainly presupposes the individual's right to control the use of that image, including the right to refuse publication thereof …"[37]

Legitimate expectation is applicable even if the person concerned was a public figure. "[E]ven if such a public interest existed, just as there existed a commercial interest for the magazines to publish the photographs and articles, those interests had .. to yield to the applicant's right to the effective protection of her private life".[38]

With the increasingly massive collection and storage of data by corporations, it is crucial that we re-think privacy. Is privacy signed away when we voluntarily provide data to corporations in order to access their services? What are the obligations of corporations who compile and store personal data? Furthermore consent, if sought, for providing data, is normally contained in long contracts published in small fonts, which in any event, is not read by most people.

Unauthorized access to and dissemination of data all cause distress, harm and damage. Yet, courts frequently do not recognize harm arising from breaches or theft of data.[39] This is because taking preventive steps to avoid or remedy foreseeable risk of future harm arising from data breaches (as opposed to actual damage or injury) is not generally a cognizable injury. Neither is emotional distress caused by exposure of data. These risks are deemed to be part of "the ordinary frustrations and inconveniences that everyone confronts in daily life with or without fraud or negligence".

That being the case, it is necessary to re-look at the business model that focuses on collection, storage and analysis of massive amounts of personal data. This is particularly critical as often, the data collected is often are disproportionate to what is required for interaction with their customers.

d) *Consent*

A criteria in determining whether a violation has occurred is consent. The DDP Paper I discusses in detail the issue of consent and differentiates between consent that is specific to an individual and consent for data or image to be shared. Personal data is no less personal even though it may be available in the public domain.[40]

Consent may also be conditional and temporal. A German Federal Court ordered a photographer to destroy intimate photos of his ex-lover after their break-up, irrespective of whether he had any intention of sharing them. The Court held the consent to have been withdrawn when their relationship ended as retaining the photos would have granted the photographer 'manipulative power' over his ex-lover.[41]

---

[37] ECtHR, Von Hannover v. Germany (No. 2), Grand Chamber judgment of 7 February 2012, § 96. This legitimate expectation is grounded in Article 8 (right to respect for private life) of the European Convention on Human Rights and its violation constitutes a violation of human rights.
[38] *Id.*
[39] *In re Hannaford Bros Co. Customer Data Security Breach Litigation*, 2010 ME 93, 4 A.3d 492
[40] Aziz, DDP Paper I, p.
[41] Sex tape row: German court orders man to destroy naked images, BBC News, 22nd December 2015, http://www.bbc.com/news/world-europe-35159187. Accessed 1 February 2018.

➢ *Anonymity*

Anonymity is a feature that has to a large extent contributed to the lively and provocative discussions on the internet. Protecting the anonymity of users has also facilitated social and political activism particularly in oppressive regimes. Experts have maintained that restrictions on encryption and anonymity tools put the privacy of all internet users at risk.[42] Anonymity is also critical for whistle-blowers, human rights defenders, victims of ICTV (both for purposes of reporting and re-entry into ICT spaces post ICTV).[43]

There is a false sense that anonymity and accountability are inversely related in that increased anonymity results in decreased accountability. Researchers have found that the anonymous nature of the internet may elevate the perception of the online disinhibition effect (see above) as, in the online environment, people are less sensitive to the consequences of their actions due to geographical and temporal distance. This may motivate the perpetration of ICT related violence. [44] However, rather than removing anonymity, the solution may lie with simultaneous implementation of anonymity protections and accountability mechanisms.[45]

In a bid to encourage users to be more responsible and abide by community standards, some platform providers require users to authenticate their identity. Executives from major Internet application companies such as Facebook and Google have defended their respective real-name policies—in which users are required to associate their online identities with their names as necessary to promote stronger accountability, the underlying assumption being that there is no other means of holding users accountable beyond stripping them of their anonymity.[46]

Following from early criticism to their authentication policy, Facebook's authentication of identity policy currently requires users to provide authentic identity, that is the identity a person is known to his/her community.[47] This name is not necessarily his/her legal identity. It also provides users whose profiles have been flagged with options to explain their situation, including, "affected by abuse, stalking or bullying" and "lesbian, gay, bisexual, transgender or queer".[48] Supported by research that indicates users are "eight times more likely to abide by [their] community standards if they have authentic names", Facebook maintains that the authentic name policy is one tool in their toolkit for "user accountability and keeping people safe" along with community standards, reporting mechanism and penalties for violating such standard.[49]

---

[42] Kaye, David, (Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinon and Expression), U.N. Doc. A/HRC/29/32 (May 22, 2015), *available at* https://documents-dds-ny.un.org/doc/UNDOC/GEN/G15/095/85/PDF/G1509585.pdf?OpenElement.

[43] Aziz, DDP Paper I, p. 10.

[44] Randy M Young & Ors, *Does gender matter in cyberbullying perpetration? An empirical investigation,* Computers in Human Behaviour, 79 (2018)247 – 257 quoting Hinduja, S., & Patchin, J. W. (2010). Bullying, cyberbullying, and suicide. Archives of Suicide Research, 14(3), 206e221. In the online environment, people are less sensitive to the consequences of their actions due to geographical and temporal distance.

[45] Wolff, Josephine, Application-layer design patterns for accountable–anonymous online identities, Telecommunications Policy 37(2013)748–756.

[46] Pfanner, E, *Naming names on the Internet*, New York Times, 4 September 2015. Available at www.nytimes.com/2011/09/05/technology/ naming-names-on-the-internet.html. Accessed 1 February 2018.

[47] DDP expert meeting, 16-17 January 2018, Washington DC.

[48] Amanda Hopuch, Facebook adjusts controversial 'real name' policy in wake of criticism, Guardian, 15 December 2015. Available at https://www.theguardian.com/us-news/2015/dec/15/facebook-change-controversial-real-name-policy. Accessed 13 February 2018.

[49] DDP expert meeting, 16-17 January 2018, Washington DC.

On the other hand, authentication processes tend to create central, identifiable databases linking all the accounts. The end result is they facilitate marketing strategies, limit the number of accounts users may have as well as provide points of access for State enforcement and surveillance requests, which arguably has its own harms.

In order to correlate accountability to identity, other researchers have suggested what is needed is to reduce the discardability of online identities and provided examples of user investment in its online identity (which could be gauged by investment of time rather than money). This means that end-users should be able to decide for themselves how much they wish to invest in their online identities and the size of that investment should then determine the privileges of that identity within the context of a given application.[50] While this solution is most beneficial to establishing and enhancing the credibility and reputation of businesses, it has net effect similar to authentication processes.

Another possibility is linking the identity across multiple applications. This will allow different applications and platforms to share information of online misbehavior. More thought is needed on whether this sharing is an appropriate response as it has the potential of amplifying the consequences to the perpetrator beyond his original act.

3. Responses to ICTV

➢ *Responses by duty-bearers*

This section looks at responses to ICTV by relevant duty-bearers as well as their obligations to eliminate ICTV.

a) Responses by States

States have an obligation to exercise due diligence to prevent and respond to gender based violence. This is comprised in both international law and domestic law including their respective constitutions.

A lot of the work on State obligation have been norm setting and norm changing. Eliminating ICTV however requires political will, expertise and collaboration with civil society and constituents. States should also identify partnerships across sectors and open and transparent consultations with all relevant stakeholders.

A research in India found that only a third of respondents of ICTV had reported online harassment to law enforcement. Of those, just 11 percent said they were helpful, compared to 51 percent who found them only somewhat helpful, and another 38 percent who said they were not at all helpful. Over half (52 percent) said that officials do not take complaints of online harassment seriously. Among them, 38 percent characterized the response as "not at all helpful."[51] That is, only 3.3% of respondents reported positive interaction with the police.

While gender-based VaW needs to be eliminated both offline and online, and much of the law, policies, processes and procedures may be equally applicable to ICTV and other forms of VaW, the specificity of information communication technology for example, its reach, its speed, the participation of secondary perpetrators,[52] the aggregated harm, the anonymity

[50] Wolff, Josephine, Application-layer design patterns for accountable–anonymous online identities, Telecommunications Policy 37(2013)748–756.
[51] *Id.* n. 5, p. 13
[52] See Aziz, DDP Paper I for discussion on secondary perpetrators, p. 10.

and the disinhibition that accompanies communications, all require some level of re-thinking and re-training.

Jurisdictional (extra-territoriality) arguments, resulting in the inability to hold actors accountable needs to be addressed. Cooperation amongst States to eliminate ICTV must be based on laws that comply with universal human rights principles. Ensuring that national laws are human rights compliant can avoid disputes about enforcement of laws that violate freedom of expression.

Another challenge is enforcement or laws and policies. The German *Law for the Improvement of Law Enforcement in Social Networks (Network Enforcement Act - NetzDG)* requires that popular social media platforms have in place effective and transparent procedures to deal with complaints.[53] The law requires platforms to remove clearly illegal content within 24 hours and within seven days if the content is ambiguous. Platforms that receive more than 100 complaints of illegal content per year must also submit a report of their handling of complaints. Breaches can be punished by fines of up to €5,000,000. This new law does not provide for criminalization of any act. It is an enforcement law with prohibitive penalties that needs more monitoring to determine its desirability and effectiveness.

States also need to protect and facilitate access to open ICTs including the internet. This should include ensuring women's access through the elimination on ICTV, and protection of women's voice and agency. Diversifying the technical community and technology industry by increasing women's involvement and participation is desirable, if not necessary to sensitize the industry to women's needs and perspectives.

Intermediaries should also report when there are laws that are overly broad and violates human rights. Although in "Fuiste Mia" ("You were mine"), State action was appropriate in the context of Mexican prevalence of femicide, repressive regimes may as easily abuse their authority to seek removal of content that are critical of the regime. Regulation and, ideally, an independent mechanism is needed to determine what content should be responded to because it constitutes hate speech even if it's not illegal. Where there is an operating judicial system, courts or special tribunals have may assume this role.

The State also needs to take proactive measures to educate and prevent ICTV. It is important to make sure that women and girls have access to learning about anonymity, encryption, and what that means for them in a way that emphasizes that they are in no way to be blamed for violence committed against them. Passwords and two-step verification, for example, are simple measures that targets of violence can be taught to implement.

"We tend think of cybersecurity as a problem for governments, major corporations, and — at an individual level — for people with credit card numbers or identities to steal. The average teenage or young-adult internet user, however, is the very softest of cyber security targets."[54]

In sextortion cases, for example, perpetrators may use malicious software, which allow the perpetrator access to all files on the victim/survivor's computer or allow the perpetrator to see everything typed on the keyboard and/or turn on web cameras and microphones attached to the camera at will.

---

[53] Law for the Improvement of Law Enforcement in Social Networks (Network Enforcement Act - NetzDG) (Federal Law Gazette I p. 3352). Available at https://www.gesetze-im-internet.de/netzdg/BJNR335210017.html. Accessed 1 February 2018.

[54] Wittes, Benjamin & Ors, *Sextortion: Cybersecurity, teenagers, and remote sexual assault*, Brookings, May 2016. Available at https://www.brookings.edu/wp-content/uploads/2016/05/sextortion1-1.pdf. Part of intermediaries' response is also to create guides such as parenting guide on online violence. For Facebook, these are located in the Safety Center, including a parenting guide on how to help with online violence. See https://www.facebook.com/safety. For parenting guide, see https://www.facebook.com/safety/parents

Once a victim/survivors comes forward, it is essential that all investigations by both the State and intermediaries is undertaken sensitively and confidentially and her anonymity is protected. This is to avoid re-victimized during investigations by the State and by intermediaries.

b) Responses by intermediaries

Postings on the internet have a level of permanence and can repeatedly be searched, accessed and disseminated, making the harm persistent. Without the intercession of intermediaries, there is no escape from ICTV unless victims are willing to disconnect from their ICT networks.[55] A reporting procedure that protects the personal data and preserves the anonymity of the victim/survivor is critical. As secondary perpetration, namely the sharing, uploading, downloading and re-transmission of illegal content such as photos, is prevalent and creates a permanent effect of ICTV, implementing measures to prevent such data and image from being shared and re-transmitted is important.[56]

Intermediary liability is clearer when dealing with illegal content, especially when there is a court order. However, a better paradigm which can exist alongside State obligation to eliminate VaW, is for intermediaries to subscribe to a new business model that holds themselves accountable because of their own human rights responsibilities. The idea that you need to have very cogent reasons to impose liability on intermediaries because they are mere conduits is now strained because categorization of intermediaries is being opened for debate. The level of editorial discretion and control exercised by some of these platforms exercise makes it difficult to categorize them as just conduits. Further, intermediaries are often no longer merely 'hosting' but providing content or at the very least are involved in prioritizing or popularizing content through tendencies to promote already-popular content. This can easily result in posts being promoted that have misinformation or that is aimed to incite gender-based violence which may slip past community standards scrutiny.[57]

The use of technology for political disinformation and terrorism has injected concern over the role of intermediaries. The debate on intermediary responsibility not to facilitate terrorism has resulted in calls for the restriction on encryption in favour of identity disclosure and surveillance over privacy. At the same time, privacy concerns have also drawn the limelight in ongoing debate about 'the right to be forgotten'.[58] These complex discussions have and will continue to influence and impact our demands for strategies on eliminating ICTV.

It is crucial that we view all forms of violence holistically and start breaking down invisible silos surrounding each form of abuse and violence. Women and experts on VaW need to be aware of these different discussions impacting violence against women and demand that women and girls be consulted and their voices, concerns and human rights be taken into consideration in the formulation of these responses.

---

[55] Cassidy, Faucher, & Jackson *Cyberbullying among youth: A comprehensive review of current international research and its implications and application to policy and practice*. School Psychology International 34(6), 575 - 612.

[56] For example, storing of the hash of the image to stop such images from being shared on other platforms.

[57] Such news feeding tendencies have resulted in, for example, misinformation and propaganda against the Rohingya which apparently avoided the community-standards scrutiny. Ingrid Burrington, *Could Facebook be tried for human rights abuses?*, The Atlantic, 20 December 2017, https://www.theatlantic.com/technology/archive/2017/12/could-facebook-be-tried-for-war-crimes/548639/. Accessed 1 February 2018.

[58] See DDP Paper I.

The allocation of legal responsibilities for regulated content forms the bulk of State regulation of intermediary liability. On the one hand you have a laissez faire approach. On the other hand you have regimes where intermediaries are under a lot of pressure to take down blacklisted sites or remove any content alleged to fall within a restricted category, including negative content about the government or politicians. In between these two is where most of the law exists. The most common framework requires intermediaries to pass on information about content that is perceived to be illegal, sometimes accompanied with take-downs.

On their part, intermediaries, including telecommunication companies, are implementing mechanisms to address these challenges, including from a human rights perspective. It is critical, though, that these actions be transparent. More data from intermediaries including platform providers on how they design and implement these mechanisms is needed.[59] After all, the intermediaries are required to walk the thin line between eliminating violence and hate speech on the one hand and paternalism on the other; and between protecting the rights of everyone to access the internet (which necessitates eliminating ICTV) and taking down content or removing anonymity due to pressures from repressive regimes in violation of freedom of expression principles.

Internet intermediaries too have responded by creating community standards as well as tools to control user experience as well as back-end tools to identify and remove violating content. It is important that such community standards and guideline are sensitive to ICTV and clearly defines unacceptable conduct constituting violence against women. Any attempt at creating global community standards must take into account women's rights and freedoms.

Still, universal application of community standards developed at headquarters in the global north may also not be sensitive to diverse social norms elsewhere. Taking the cue from complaints of difficulty in accessing intermediaries' complaint mechanisms due to cultural, language and legal barriers,[60] intermediaries report that they are working to make sure everyone has access, and that the translators have actual native, local speakers.[61]

Understanding differences in local social and cultural norms also mean perceived transgressions of social and cultural norms, have difference consequences in different countries. For example, in some countries, slut-shaming, that is criticizing women and girls whose behaviour, sexual expression or opinions transgress social expectations, may result in women being subjected to violence, even murder, for defying these social and cultural expectations.[62]

It is however critical that all relevant stakeholders, the State, internet intermediaries, the technical community, civil society and the academia collaborate in developing preventive measures and policies, as well as laws on ICTV.[63] Such policies and laws must be principled, explicable and enforceable.

Reliance on algorithms to filter and remove non-compliant content is problematic and insufficient due to 'biased learning'. Yet, it is not that machine learning is biased. Rather,

[59] Intermediaries report that they are working on releasing data but have to first ensure that such data will not be confusing due to variation in terminology, particularly terminology used in complaints. For example, while a report may specify bullying but in fact, is more accurately defined as harassment. DDP expert meeting, 16-17 January 2018, Washington DC.
[60] Digital Rights Foundation, Helpline report, p.16
[61] Facebook currently have policies to ensure that their reviewers understand local contexts and sensitivities.
[62] *Pakistani model Qandeel Baloch killed by brother after friends' taunts – mother*, The Guardian, 27 July 2016. Available at https://www.theguardian.com/world/2016/jul/28/pakistani-model-qandeel-baloch-killed-by-brother-after-friends-taunts-mother
[63] For example, Facebook launched #HerVoice, a safety policy training program for NGOs and policy makers on building strong social media campaigns to help address online harassment of women.

machine learning exposes the bias, sexism and racism that still exist in society and the media today. For example a system trained with existing news will adopt the very bias of the news articles. "Statistically, the statements are correct using just what can be derived from the articles. But the articles themselves are obviously biased."[64] What is required are algorithms that are discerning and accountable. More gender sensitive designers, including more women and gender non-conforming designers are needed to recognize gender biases and ensure that algorithms do not adopt these biases. In addition, the ability to explain the data sets being used by the algorithm and the determinations being made will ensure that we do not escape the world of human accountability.

Finally any self-regulatory model must be accompanied by enforcement procedures. So far, there is no effective enforcement procedure. Furthermore, corporations are free to decide how much time, money and other resources they are willing to provide to eliminate VaW. Based on a business for profit model, more self-regulatory mechanisms will be put in place where violations would be economically or financially detrimental. Violations of intellectual property, for example has cost intermediaries millions in damages whereas the cost of ICTV is so far rather invisible and therefore wont not to receive the same level of attention.

c) Independent mechanism

In the context of ICTV, is it better for states to decide when content should be illegal, or is it better for companies? When it is characterized as illegal in one country what is the appropriate way of taking it down? Will that affect only the people in that country or will it have broader implications? What does due process mean vis a vis a company process? What do you do about content that is problematic but we want to make sure it's still available, or content that must be taken down? Is there some alternative to leaving the decision up to governments or platforms?

The German law on networking may result in compelling platforms to err on the said of taking down content rather than face hefty fines.[65] Facebook, for example, has hired (directly or indirectly) thousands of people to delete hate speech.[66] Critics opine that this gives platforms too much power to interpret the legislation (or, in lieu of legislation, the uncodified wishes of legislators and regulators) or cause platforms to take down more content than they should for fear of hefty fines or burdensome regulations.[67] In the extreme, this can lay the foundation for non-transparent if not secret form of censorship. Some kind of oversight is clearly required and careful monitoring of the German law will provide the opportunity for stakeholders to work on ensuring human rights are respected in these processes.

For various structural and functional reasons, there is merit in the argument that neither institution, the State and internet intermediaries, should be regulating ICT on their own but that we should consider establishing another mechanism. An independent mechanism may also overcome jurisdictional and territorial issues to facilitate universal enforceability. Of course, in considering if an independent third party mechanism is the answer, questions on governing

---

[64] Yvonne Baur, Is machine learning biased? Tech Crunch, 11 October 2016. Available at https://techcrunch.com/2016/10/11/is-machine-learning-sexist/. Accessed 1 February 2018.
[65] *Supra* n. 51.
[66] See also above discussion on the problems of using algorithms to deal with hate speech. Still, Facebooks long-term solution is to build AI technology to automatically detect violent or inappropriate posts, pull them down or stop them from going up in the first place. Kurt Wagner, *Facebook is hiring another 3,000 people to pull down violent and inappropriate content,* Recode, 3 May 2017. Available at https://www.recode.net/2017/5/3/15531478/facebook-hiring-3000-people-violent-inappropriate-video-content-post
[67] Facebook to hire 500 workers in Essen to delete hate speech, The Local, 9 August 2017. Available at https://www.thelocal.de/20170809/facebook-to-hire-500-employees-in-essen-to-combat-hate-speech-socialmedia.

structure, access to information, enforcement procedures and resources will need to be carefully thought out. In such a diverse ecosystem that is the ICT, these processes must work for all parties concerned and not overly punish small industry actors and stakeholders.

d) Responses by Users

Increasing the role of users is a worthwhile consideration provided this does not result in laying blame on women and victims/survivors for the violence perpetrated against them. Many of the lessons learnt by advocates in eliminating off line violence are similarly applicable in ICTV.

Responses can include special helpline to report ICTV as was undertaken in India and Pakistan.[68] In terms of solutions, we need to look at what can be done to strengthen women to fight back. For example, the biggest state in India set up a special helpline to report ICTV in 2012.

Support groups may also be formed using ICT. For example 'Circle of 6' is a mobile phone application to prevent sexual violence. It allows a user to discreetly and quickly seek help ("come and get me") or interruption ("call and pretend you need me") by tapping on her phone. The application will automatically contact persons pre-programmed into the application with the user's GPS location.[69]

Unlike most offline VaW, online VaW is witnessed by thousands of users. As harm may be caused by collective action of perpetrators and secondary perpetrators, it is possible to garner bystander intervention or collective action online in empowering victims/survivors to 'fight back'. Counter-speech may also push discourse norm and stop others from perpetrating hate speech.[70]

The #MeToo movement, for example, was popularized to provide victims/survivors a voice and to demonstrate the magnitude and prevalence of violence against women. It is based on the concept of empowerment through empathy. [71] It serves as a "bold declarative statement that 'I'm not ashamed' and 'I'm not alone.' On the other side, it's a statement from survivor to survivor that says 'I see you, I hear you, I understand you and I'm here for you or I get it." [72]

Hollarback! is another movement built on collective action. It leverages on technology to end street harassment, using " the very spaces where harassment happens – from online to the streets – to have each other's backs, create communities of resistance, and build a world where we can all be who we are, wherever we are."[73]

All these are examples of user, particularly women creating their own spaces and exercising freedom of expression to combat ICTV, laying the first firm steps towards achieving the internet and ICT spaces that is inclusive, equal and diverse.

---

[68] Ibid n. 5. See also *Cyber Harassment One Year Report, December 2017 – November 2018*, Digital Rights Foundation, 2018. Available at https://digitalrightsfoundation.pk/wp-content/uploads/2017/12/Helpline-Annual-Report.pdf

[69] Circle of 6. Available at https://www.circleof6app.com/

[70] See above examples of Mexican musicians reaction after State and public action.

[71] Tarana Burke, as quoted in Cassandra Santiago and Doug Criss, *An activist, a little girl and the heartbreaking origin of 'Me too'*, CNN, 17 October 2017. Available at http://www.cnn.com/2017/10/17/us/me-too-tarana-burke-origin-trnd/index.html

[72] *Id.*

[73] https://www.ihollaback.org/about/