



End violence: Women's rights and safety online

**Exploring corporate and state remedies for technology-
related violence against women**

Research design

Rima Athar and Women's Legal and Human Rights Bureau, Inc.

*Association for Progressive Communications (APC)
November 2013*

This research is part of the APC "End violence: Women's rights and online safety" project funded by the [Dutch Ministry of Foreign Affairs \(DGIS\)](#) and is based on a strong alliance with partners in seven countries: Bosnia and Herzegovina, Colombia, the Democratic Republic of Congo, Kenya, Mexico, Pakistan and the Philippines. For more information visit [GenderIT.org](#) and [Take Back the Tech!](#)

Table of contents

I. Theoretical framework

1. Introduction.....	3
1.1. Background	3
1.2. A framework for mapping technology-related VAW.....	3
1.3. Interplay between offline and online violence.....	5
2. Common types of rights violations	6
3. Understanding harm in relation to technology-related VAW.....	7
4. Key stakeholders.....	9
5. Exploring legal remedies	9
5.1. Providing legal remedy in cases of technology-related VAW.	9
5.2. Areas for further research.....	11
6. Exploring corporate remedies.....	11
6.1. Liability issues and concerns.....	11
6.2. Corporate responsibility and international human rights.....	13
6.3. Corporate responsibility in regards to VAW.....	13
6.4. Existing responses and interventions.....	14
7. Works cited.....	17

II. Research design

1. Research as an output of the FLOW/EndVAW project.....	20
2. Research goals	20
3. Case study methodology and corresponding activities.....	21
4. Criteria for selecting cases	23
5. Indicators for analysis.....	25
6. Overarching research matrix.....	28
7. Ethics in the research process.....	30
8. Key terms, concepts and definitions.....	37

III. Research instruments

1. Check list for mapping domestic legislation.....	44
1.1. Check list.....	44
1.2. Contextual background and critical analysis of national legislation.....	46
2. Check list for mapping corporate user policies.....	47
3. Informed consent form for victims/survivors.....	49
4. Semi-structured interviews of victims/survivors.....	51
4.1. Background to the Interview.....	51
4.2. Interview questions.....	52
5. Semi-structured interview for law enforcers involved in the case.....	60
6. Semi-structured interview with NGOs involved in the case.....	61
7. Semi-structured interviews with internet intermediary representatives	62
8. Template for case study write-up.....	66
9. Guidelines for conducting the interview with VAW victim/survivor.....	68

I. Theoretical framework

1. Introduction

1.1. Background

The proposed research is part of the “End violence: Women's rights and safety online” (EndVAW) project to be implemented from 2012 to 2015 by the Association for Progressive Communications (APC), with support from the Dutch government’s Funding Leadership and Opportunities for Women (FLOW) programme. The project builds on APC’s experience in the anti-VAW struggle and existing partnerships to enhance women's safety by preventing the incidence of technology-related violence against women.

The project targets women leaders – women's rights advocates, women in the technology industry, community activists, young women peer leaders and opinion-makers – as well as women's rights organisations that are already active in implementing interventions and advocacy strategies to address technology-related VAW.

The project’s activities are carried out in collaboration with country partners in Mexico, Colombia, the Democratic Republic of Congo (DRC), Kenya, the Philippines, Pakistan and Bosnia and Herzegovina, as well as globally through campaigning and advocacy.

Since 2005 APC has strengthened the capacity of women’s rights activists and organisations to use technology tools in their work to end violence against women and to respond to the growing incidence of technology-related violence against women. Through a three-year project (2009-2011) in 12 countries in Africa, Asia and Latin America, APC established that the most common violations were cyber stalking, sexual harassment, privacy violations, surveillance and the unauthorised use and manipulation of personal information including images and videos. We found that in all of the 12 countries, policies, regulations or services to prevent or respond to these new forms of violence do not exist or are inadequate. *Women and girls who fall victim do not know what to do to stop the abuse, what charges they can report, who they should report to and what help they can get.* A key learning from our work over this three-year project is that we need to examine availability and effectiveness of existing legal and civic remedies for victims/survivors technology-related VAW and to prevent such violence.

1.2. A framework for mapping technology-related VAW¹

Although VAW has its roots in gender inequality in all societies and cultures, across the world, the way in which it manifests depends on the specific social, economic, cultural and political context. Consequently different or new forms of VAW may increase or arise when societies undergo demographic, political and economic changes, or social and cultural shifts. This includes when new ICTs enter the scene.

Technology-related VAW is a distinct phenomenon because of the medium, mode and place of its commission. The context in which it manifests remains relatively unexplored and less understood and as such has implications on women’s access to justice. The distinct characteristic of ICT – its borderless

¹ This framework for mapping technology-related VAW is culled from APC’s previous research conducted under its MDG3: Take Back the Tech programme (2009-2012), as well as the Women’s Legal and Human Rights Bureau-Philippines’ unpublished paper titled, “Study on ICT, VAW and Sexuality: A Policy Advocacy”.

nature, the fluidity of digital personhood,² the absence of physicality, and the anonymity and intractability it offers – has changed not only the manner by which VAW is being committed and perpetrated, but also its effects and consequences, and its subsequent prosecution or non-prosecution.

Between 2009-2012, APC implemented its first multi-country programme “MDG3: Take Back the Tech” in 12 countries in Africa, Asia and Latin America, with the aim of mapping how online and mobile technologies are being used to perpetrate acts of VAW.³ Technology-related VAW was seen as connected to existing and recognised forms of violence against women, including:

- *Harassment and stalking*, which constitutes one of the most visible forms of technology-related VAW. This ranges from harassing SMS messages and online comments to tracking women’s networks, friends, movements and activities through mobile phones, social networking spaces like Orkut, and geolocation tools. It is important to note that the line when harassment crosses over into stalking may be hard to qualify. According to UK’s National Stalking Helpline: “If the behaviour is persistent and clearly unwanted causing you fear, harassment or anxiety then it is stalking and you should not have to live with it.”⁴
- *Intimate partner violence*, where technology is used in acts of violence and abuse in intimate or spousal relationships. For example, women are afraid to leave abusive relationships due to threats by their partners of disclosure of private and intimate communications by their partners.
- *“Culturally justified” violence against women*, where culture or religion is used as a reason to justify, ignore, or accept acts of VAW, or when technology plays a role in creating a culture of VAW. It can be something as thoughtless as forwarding a sexist joke that supports the idea that women are less valuable than men or suggesting that when women say no, they really mean yes, to starting a Facebook group that promotes different ways to rape girlfriends.
- *Rape and sexual assault*, where technology is used to track the movement and activities of a victim/survivor, to provide location information, or when an act of violence is digitally recorded and distributed. In other cases, the internet is used to lure women into situations of sexual assault.
- *Violence targeting communities*, where communities face targeted online attacks and harassment because of their gender, sexual identity or political views. For example, the websites of many women’s rights organisation have been hacked because of their stance on gender equality and feminism. Women bloggers who are outspoken about discrimination have also faced overwhelming attacks and messages that aim to disrupt their ability to express themselves online.⁵

In practice, the violence a woman experiences may overlap across these categories. Research also demonstrated that a combination of factors affect the prevalence and manifestations of technology-related VAW. This includes:

- Who the perpetrators are (e.g. intimate partners, parents, strangers, community, state)

² Gurumurthy, A., & Menon, N. (2009, 3 October). Violence against Women via Cyberspace. *Economic & Political Weekly (EPW)*, XLIV(4).

³ For an overview report on the findings of the MDG3: Take Back the Tech programme (2009-2012), see: Fialova, K., & Fascendini, F. (2011). *Voices from Digital Spaces: Technology related violence against women*. APC. www.genderit.org/node/3539; for country-specific reports, see: www.apc.org/en/node/10360

⁴ www.stalkinghelpline.org/faq/about-stalking

⁵ Cases of this nature are discussed below in the section on exploring corporate legal remedies.

- The technology platform used by perpetrators (e.g. mobile phone, social networking platforms, chatting, email, website, webcam)
- The nature of the violence (e.g. online harassment and stalking, intimate partner violence, “culturally justified” violence, sexual assault and rape, violence targeting particular communities)
- The type of violence act (e.g. threats, blackmail, stealing someone’s money or property, identity theft, surveillance of online and/or offline activity, unauthorised recording and/or distribution)
- The harm faced by the victim/survivor (e.g. physical harm, psychological harm, sexual harm, economic harm, or privacy harm)
- The social and bodily characteristics of the victim/survivor (e.g. class, ethnicity, nationality, race, age, or physical and intellectual abilities).

Another distinction can be made in how technology-related VAW is perpetrated:

1. Technology is a tool in the perpetrators hands to carry out acts of violence against women, either online or offline, or both (taking/uploading a video, photo-shopping a photo, blackmail). The victim/survivor doesn’t necessarily know of/come into contact with the technology themselves.
2. A woman’s use of technology is targeted by others as a way to harass/intimidate/cause harm (e.g. harassment directed at her Facebook/Twitter/email account; or she receives threatening text messages or WhatsApp messages; her private data is collected from hacking into her computer; monitoring and tracking her whereabouts, etc.).

The above findings sketch a broad picture of how technology-related VAW occurs. This research aims to go the next step and explore individual cases in-depth to help refine the bigger picture and to develop context-specific advocacy strategies for appropriate legal and civic remedies.

1.3. Interplay between offline and online violence

The UN Declaration on the Elimination of Violence Against Women (DEVAW) defines violence against women (VAW) as “any act of gender-based violence that results in, or is likely to result in, physical, sexual or psychological harm or suffering to women, including threats of such acts, coercion or arbitrary deprivation of liberty, whether occurring in public or in private life.”

As stated by APC’s statement to the 57th session of the Commission on the Status of Women:⁶

Violence against women that is mediated by technology is increasingly becoming part of women’s experience of violence and their online interactions. In the same way we face risks offline, in the streets and in our homes, women and girls can face specific dangers and risks on the internet such as online harassment, cyber stalking, privacy invasions with the threat of blackmail, viral “rape videos” and for young women in particular, the distribution of “sex videos” that force survivors to relive the trauma of sexual assault every time it is reposted online, via mobile phone or distributed in other ways.

⁶ Association for Progressive Communications (APC). (2013). Statement to the 57th Session of the CSW: Violence against women and information and communications technology. www.apc.org/en/pubs/statement-57th-session-csw-violence-against-women

These forms of violence may also be mediated through technology but they cause psychological and emotional harm, reinforce prejudice, damage reputation, cause economic loss and pose barriers to participation in public life.

Yet the absence of physical contact in digital spaces is often used to minimise the importance of attacks on women's bodily integrity made online or using mobile technologies. Most laws and policies that address violence against women limit their definitions of harm to physical harms alone, and as the UN Secretary General highlights in his 2006 report, neglect the emotional and psychological aspects of abuse when creating and implementing legal standards as well as their implementation. The UN report calls for greater attention "to the use of technology, such as computers and cell phones, in developing and expanding new forms of violence. Evolving and emerging forms of violence need to be named so that they can be recognised and better addressed."⁷

Six years later, despite evidence showing an increase in violations involving technology, there has been little recognition of technology-related forms of violence against women by states, intergovernmental institutions, and other actors engaged in efforts to end violence against women. It is not prioritised in prevention and response strategies, or budgeting and evidence-based policy making, and women who experience these violations have no recourse of redress.

This research seeks to contribute to a deeper understanding of the interplay between emotional, psychological, physical and socio-economic harms faced by women; to analyse the barriers to/opportunities for effective legal and civic remedies to provide redress and protect women's rights; and to develop advocacy materials towards this end.

2. Common types of rights violations

The observations and findings of the MDG3: Take Back the Tech programme showed the following to be the most common ways that rights violations happen through use of technologies:

- **Accessing private data**
Accessing your private information without consent, by hacking into your account, stealing your password, using your computer to access your accounts while it is logged in etc.
- **Taking photos/video without consent**
Taking photographs or recording videos of you without your knowledge or consent.
- **Sexual assault and rape videos**
Filming acts of sexual assault and rape, and distributing these through networked devices and online platforms.
- **Monitoring and tracking**
Monitoring & tracking your online or offline activities and movement.
- **Deleting, changing or faking personal data, photos/videos**
Deleting your emails, creating false personal data like online accounts or advertisement postings, manipulating or creating fake photos and videos of you.

⁷ UN Secretary General. (2006). In-depth Study on All Forms of Violence Against Women (A/61/122/Add.1/Corr.1). daccess-dds-ny.un.org/doc/UNDOC/GEN/N06/419/74/PDF/N0641974.pdf?OpenElement

- **Repeated harassment**
Repeated and unwanted harassment through messages, contact, publishing info about you online etc.
- **Threats of violence/blackmail**
Sending threatening messages or blackmailing you with threats of publishing personal photographs online etc.
- **Stealing identity, money or property**
Stealing your identity by creating a fake account under your name, using your passwords to withdraw money from your bank account, etc.
- **Sharing and/or disseminating private information**
Sharing and/or disseminating private information & communication like videos, photos and emails, without your knowledge or consent.
- **Abusive comments**
Offensive or denigrating online comments meant to hurt a person's reputation or diminish her/his work, content production, etc.

3. Understanding harm in relation to technology-related VAW

The harms and other consequences that victims/survivors of technology-related violence against women suffer are very often diminished or disregarded in the heated public debates accompanying such incidents. Technology-related violence usually takes place online and unless it extends to the physical world, it mostly results in psychological and emotional harm, rather than physical violence. Harm can be either subjective (the fear of being harmed, for example) or objective (such as harassment or stalking). As yet, while some courts recognise objective harm, the subjective harm, for example of privacy violations is largely unrecognised.

APC's mapping shows that the harms resulting from technology-related VAW include:

- Emotional or psychological harm
- Harm to reputation
- Physical harm
- Sexual harm
- Invasion of privacy
- Loss of identity
- Mobility limited
- Censorship
- Loss of property.

These harms are not mutually exclusive, and multiple harms are often simultaneously experienced. For the purposes of this research we understand harm to constitute a part of violence. We recognise that violence occurs on a spectrum and ranges in severity by which it is experienced; e.g. from discomfort to harm to abuse to violence. Yet this spectrum is not necessarily linear, and the 'severity' is often hard to objectively discern; for example, repeated and prolonged discomfort and harm is precisely a technique

used to inflict psychological and physical abuse and violence, sometimes amounting to torture. With specific regard to ICTs and sharing through networked devices, videos or photos of violent acts being continuously circulated, commented on and repeatedly viewed cause repeated harm to the survivor and constitute secondary victimisation and new acts of violence.⁸ As Anastasia Powell argues, “The unauthorised taking and distribution of images of an otherwise consensual sexual encounter is similarly part of a continuum of gendered sexual violence and harassment targeting primarily women, where the distribution is itself a violation of an individual’s sexual autonomy with the effect of humiliating, intimidating or otherwise harassing the victim.”⁹ This also brings into question the role of actors – beyond the initial perpetrators of violence – in legitimising and enacting VAW, in blaming and shaming victims/survivors, and in hindering access to justice for victims/survivors, particularly when there is no possibility of “forgetting” an act of violence once it is circulated and documented online.

While we use the term victim/survivor in this research brief – drawing from common terminology in the discourse on violence against women – we recognise that those who experience different forms of technology-related VAW may not identify as either victims or survivors. In seeking women’s own voices and stories of their experiences in at least some of the cases being documented, this research aims to explore the way harm is experienced and defined by those whose rights have been violated, how they self-identify and respond, and thus how to create appropriate remedies that effectively recognise the specificity of such harms and their impacts. Taking a rights-based approach to technology-related VAW, and identifying which universally recognised rights are being violated, in addition to the rights provided in national constitutions and legislative frameworks, is an important entry point for awareness-raising amongst all stakeholders and for advocacy.

Understanding harms is also linked to a framework of sexual rights and sexual citizenship. At the root of gender-based violence – be it against women, men, trans- or third-gendered people – lies a perception of “appropriate” sexuality and gender-expression, based on restrictive, heteronormative patriarchal ideals. These ideals are not “natural”, or pre-ordained. They are actively constructed and mediated through the discourses people create and the actions they take to manifest these discourses, which are in turn institutionalised through legislative and normative frameworks. In the case of gender-based violence, these legislative and normative frameworks set up a mode of governing sexual citizenship. When technology is used to perpetrate VAW, it requires examining the broader cultural impacts of how heteronormative and patriarchal cultures of misogyny, hypermasculinity and hypercommodification are being actively created and embedded in our uses of technology, in our expectations of the norms governing the digital public sphere, and in our approaches and challenges to what behaviour is seen as “normal” and further “normalised” in digital spaces. Because digital technologies and the digital public sphere disintegrates a binary understanding of “public vs. private” actions, VAW committed through digital technologies and the responses of stakeholders (the state, corporate actors, perpetrators of violence, individuals and communities, etc.) are indicative of the discourses and power relations governing sexual citizenship – i.e. who is granted sexual citizenship, what rights and responsibilities are

⁸ APC started a campaign entitled “I Don’t Forward Violence” (<https://www.takebackthetech.net/take-action/2011/02/25>) in 2011 to encourage people to stop passive consumption of violent acts, and to recognise the act of sharing photos or videos of violence as contributing to a culture of normalising violence online, and even as an act of violence itself.

⁹ Powell, A. (2009). *New technologies, unauthorised visual images and sexual assault*. Australian Institute of Family Studies. www.aifs.gov.au/acssa/pubs/newsletter/n23pdf/n23c.pdf

embedded in our understandings of sexual citizenship, and what forms of control and resistance occur, both offline and online.

4. Key stakeholders

The key stakeholders and potential allies in the struggle to end technology-related VAW include:

- Users of technology (people of all genders)
- Women's rights advocates, NGOs and social service providers,
- Academics, researchers, and civil rights groups engaging issues of VAW, privacy, human rights, hate speech, etc.
- Regional and state mechanisms focused on women's issues,
- Legislators and legal professionals (judges, lawyers, formal courts)
- Law enforcement (police, cybercrime units, etc.)
- Corporate agents (i.e. leaders and staff responsible for setting and implementing policies) of internet intermediaries
- Community/informal mechanisms (neighbourhood watch, community elders, religious leaders, etc.)
- Media
- UN mechanisms and special procedures.

It is the actions of feminist users of technology, women's rights advocates, academics, researchers – as individuals and members of civil society – that are leading the struggle against technology-related VAW. Their actions and interventions include creating a counter-culture to online harassment and stalking, documenting the extent of the phenomena, calling for explicit recognition of these new forms of VAW, creating the theoretical frameworks to connect women's rights and human rights, reclaiming technology for education and prevention, creating alliances across sectors, and more. Documenting and sharing the strategies and successes of such key actors is an essential step towards ending technology-related VAW. Yet what has received less attention up to now is the responsibility of both state and corporate actors to act with due diligence to help prevent technology-related VAW, and to respond to it once violence has occurred. It is acknowledged that legislation only goes so far; but where technology facilitates the perpetuation of violence against women, there need to be appropriate mechanisms in place to provide remedy and redress.

New research is needed to explore the roles and responsibilities of legislators and legal professionals, state law enforcement mechanisms, and corporate agents in both enabling and challenging technology-related VAW.

5. Exploring legal remedies

5.1. Providing legal remedy in cases of technology-related VAW.

There is little research on the subject of technology related VAW and the law in the seven countries included in this study. Accordingly, little is known about what if any remedies or interventions are possible to prevent VAW and to provide redress for victims in these countries.

Generally, the main challenges to providing redress in cases of technology-related VAW revolve around:

- Identifying and defining technology-related VAW within national legislations
- Clarifying issues of jurisdiction
- Affording/providing protection for women against these forms violence.

As APC's MDG3: Take Back the Tech programme has noted, the struggle that victim/survivors of technology-related violence experience in seeking justice and claiming their rights revolves primarily around (a) women and girls themselves not knowing what legislation could be used to protect their rights and provide redress, and (b) legal and regulatory mechanisms and law enforcement bodies also remaining uncertain of what laws to apply and what new legislation deserves to be passed.

Based on review of studies and pertinent literature, it appears that while anti-VAW laws, cybercrime bills and law on privacy rights might be applied to cases of technology-related VAW, whether these laws are in fact applicable remains in question. Generally, the difficulty in prosecuting technology-related VAW often lies in trying to apply existing legislation to a technology that did not exist at the time the laws were drafted.

Some countries are taking up the challenge. In the Philippines, for example, the 2009 Anti-Photo and Video Voyeurism Act expressly recognises ICTs such as VCD/DVD, internet, mobile phones and similar means or devices as integral to the commission of the crime of *photo and video voyeurism*. The Anti-Child pornography Act of 2009 considers computer-generated, digitally crafted images or graphics representing a child. The Anti-trafficking in Persons Act covers cyber trafficking and cyber sex dens. The law on sexual harassment includes sending smutty jokes through text, electronic mail or other similar means.

The existence of suitable legislation is only one part of the process of providing protection to women in cases of technology-related VAW. These newer laws need to be tested for their ability to provide legal remedy. As well, the implementation and enforcement of rights guaranteed by the national legislations largely depends on the political, economic and social context of each country. Specific contexts present different challenges and opportunities for the way anti-VAW legislation impacts women.

For example, the anti-VAW laws in most countries in this study appear to have a very narrow conception of VAW. They largely look at women as victims in need of protection. The perception of VAW as a morality issue rather than as discrimination against women reinforces to control female sexual behaviour and punishes women that transgress sexual norms, even when these norms apply unequally to women and men. This has been a point of contention in the proliferation of Anti-Pornography laws which have often been manipulated to censor free expression of sexuality by women's and LGBT both offline and online. Culture and morality are often invoked as a justification to limit women's bodily and sexual autonomy and to allow many forms of VAW to continue with impunity. For instance in DRC and Kenya, the sexual violence Acts do not recognise sexual violence within marriage or domestic violence as an offence. This affects women victims/survivors of violence by their intimate partners in seeking redress; meanwhile data demonstrates that intimate-partner sexual violence is the most pervasive form of violence against women.

These observations outline possible barriers to women's access to justice in cases of VAW. In-depth exploration through case studies will substantiate which barriers are actively present for women and girls in their local contexts.

5.2. Areas for further research

There is a need to survey legal frameworks around technology-related VAW; but there is also a need to look beyond legislation to the mores and social norms surrounding their implementation (or lack thereof) and perceptions regarding women's rights and integrity. Doing so will enable advocates to:

1. Consolidate knowledge on the various substantive national legislations that exist (Constitutions, Penal Codes, Privacy Laws, anti-VAW laws, Cybercrime Bills, etc.) that have been or could be used in cases of technology-related VAW.
2. Identify both effective and problematic¹⁰ legislation.
3. Disseminate research findings about effective legal frameworks widely to make them accessible women and girls and their advocates, and facilitate women's access to justice.
4. Create evidence-based recommendations for modifying existing legislation or developing new legislation to help prevent technology-related VAW in study countries.
5. Help prepare materials to support training and capacity-building initiatives in the study countries directed at law enforcement and judicial agents responsible for policing and prosecuting cases of technology-related VAW.

6. Exploring corporate remedies

6.1. Liability issues and concerns

The role internet intermediaries play in relation to technology-related VAW needs to be considered in terms of both *liability* (legal obligations) and *responsibility* (demonstrating ethical leadership).

Intermediary liability can occur around issues such as: copy right infringements, digital piracy, trademark disputes, network management, spamming and phishing, "cybercrime", defamation, hate speech, child pornography, "illegal content", offensive but legal content, censorship, broadcasting and telecommunications laws and regulations, and privacy protection. Generally, the liability of internet intermediaries in cases of technology-related VAW, though not expressly stated, can be found under the penal codes, data privacy laws, information and communications laws, and e-commerce or electronic transactions acts of countries under study. There also exist some institutions relevant to intermediaries in some countries such as communications commissions or national telecommunication commissions.

These laws mandate that intermediaries are responsible for filtering, removing and blocking content that is considered illegal; and an argument could be made that intermediary liability is one strategy for dealing with certain real problems of unlawful content on the internet – for example to curb and control child pornography, hate speech or piracy of copyrighted material. However, when taking a more macro-

¹⁰ From a critical feminist lens, problematic legislation may be qualified as those laws which may contribute to paternalistic protectionism and censorship that actually limits women's and marginalised communities' rights (e.g. may criminalise sexuality, infringe on freedom of expression, actually limit women's critical participation and freedom of assembly in online spaces, etc.).

view of intermediaries' liability, particularly in relation to human rights, the lack of a regulatory framework for intermediaries' liability is heralded as a key pillar in the struggle for maintaining a free and open public sphere through the internet.

Prominent internet freedom organisations like Article 19, the European Digital Rights Initiative, the Electronic Frontier Foundation and the Centre for Internet and Society, all promote the concept that internet intermediaries should be immune from liability for any content hosted on their sites. The Special Rapporteurs on freedom of expression for the UN Human Rights Council, the Organization of American States, and the Organisation for Security and Cooperation in Europe have all argued that protecting freedom of expression means that "no one who simply provides technical Internet services... should be liable for content generated by others."¹¹

APC's 2012 exploratory study on the issue of intermediary liability across Nigeria, Kenya, South Africa and Uganda¹² has also highlighted the potential consequences of increasing intermediaries' liability. For example, the threat of liability may prevent the development of user-generated content platforms and social networks, resulting in adverse effects on freedom of speech and freedom of association. If intermediaries, rather than the courts become responsible for determining what content is lawful and what content is not, this may undermine the right to a fair trial or due process. Equally pernicious is the potential for governments to use intermediary liability as a means of political control and censorship, abdicating state responsibility and imposing it on intermediaries' as third parties. Thus increased liability of intermediaries may effectively undermine the democratic force and potential of the internet.

However, as Carly Nyst explains:

There is a clear and important need for intermediaries to play a more active role in ensuring that they are not complicit in, and are combatting, the use of their platforms for the perpetration of gender-based harassment and incitement to violence against women. In a context in which there are deeply ingrained gendered assumptions that result in the diminishing of women's free expression rights in favour of broader claims to free speech, and where the concept of hate speech is a subjective and often manipulated one, what role can intermediaries play in both facilitating women's free speech while enabling them to access the internet in an environment free from violence and harassment? One way to negotiate these competing concerns is by moving from an approach that focuses on the *liability* of intermediaries, to one which focuses on their *responsibility*.¹³

¹¹ Organization of American States (OAS). (2011, 1 June). Freedom of Expression Rapporteurs Issue Joint Declaration Concerning the Internet. <http://www.oas.org/en/iachr/expression/showarticle.asp?artID=848&IID=1>

¹² Comminos, A. (2012). *The liability of internet intermediaries in Nigeria, Kenya, South Africa and Uganda: An uncertain terrain*. APC. <http://www.apc.org/en/node/15649>

¹³ Nyst, C. (2013, 16 November). Internet intermediaries and violence against women - towards intermediary responsibility. *GenderIT.org*. <http://www.genderit.org/feminist-talk/towards-internet-intermediary-responsibility>

6.2. Corporate responsibility and international human rights

The “Protect, Respect and Remedy” Framework¹⁴ promoted by the UN Human Rights Council (UN HRC) was one of the first milestones in addressing the responsibility of corporations to respect human rights, put forth in 2008. It rests on three pillars:

1. The state’s duty to protect against human rights abuses by third parties, including business, through appropriate policies, regulation, and adjudication.
2. The corporate responsibility to protect human rights, which means to act with due diligence to avoid infringing on the rights of others and to provide redress when adverse impacts occur.
3. Greater access by victims to effective remedy, both judicial and non-judicial.

In order to integrate a gender-perspective into the framework, Realizing Rights: The Ethical Globalization Initiative convened a small group of experts in 2009,¹⁵ who produced recommendations on how corporations can reduce gender-based inequalities in their operational policies. Amongst the recommendations by the group:

It was suggested that corporations integrate gender analysis into assessments of their core impacts. For example, each aspect of the human rights due diligence process proposed by the SRSO [Special Representative of the UN Secretary-General] needs to be operationalized keeping in mind the need to eliminate gender discrimination and inequality. Specific steps to consider include: including indicators related to gender in evaluating corporate culture; considering gender issues in corporate governance (such as female representation on company boards); emphasizing gender in stakeholder relations; and engaging gender experts in tracking and reporting performance.¹⁶

Other international instruments provide guidance on private sector responsibility include the OECD Guidelines for Multinational Enterprises, and the Council of Europe’s Internet Governance Principles. There are also two UN special procedures mechanisms – the Working Group on business and human rights, and the Working Group on human rights and transnational corporations. Unfortunately, these mechanisms do not address gender justice or women’s rights explicitly. Research findings could be directed towards these mechanisms to help integrate such a perspective in their ongoing work.

6.3. Corporate responsibility in regards to VAW

In 2010, on the occasion of the International Day for the Elimination of Violence against Women (25 November), UN Secretary General Ban Ki-moon released a statement commending progress made in the

¹⁴ The framework was “developed by the Special Representative of the Secretary-General on the issue of human rights and transnational corporations and other business enterprises. The Special Representative annexed the Guiding Principles to his final report to the Human Rights Council (A/HRC/17/31), which also includes an introduction to the Guiding Principles and an overview of the process that led to their development. The Human Rights Council endorsed the Guiding Principles in its resolution 17/4 of 16 June 2011.” See: UN OHCHR. (2011). *Guiding Principles on Business and Human Rights: Implementing the United Nations “Protect, Respect and Remedy” Framework*. http://www.ohchr.org/Documents/Publications/GuidingPrinciplesBusinessHR_EN.pdf

¹⁵ See UN SRSO on Human Rights, Transnational Corporations and Other Business Enterprises. (2009). *Integrating a Gender Perspective into the UN “Protect, Respect and Remedy” Framework: Consultation Summary*. <http://www.reports-and-materials.org/Gender-meeting-for-Ruggie-29-Jun-2009.pdf>

¹⁶ Ibid., p. 5.

corporate sector to make women's rights a central part of their operating agenda, "from developing projects to providing direct financial support to organizations working to end violence and embracing the principles of corporate social responsibility."¹⁷

One of the more prominent global initiatives has been the "Women's Empowerment Principles" (WEP)¹⁸ which corporations can sign onto through the UN Global Compact. Signing entails recognition of the costs of violence against women to businesses, and a commitment to developing internal and external initiatives to increase women's empowerment. As of 17 April 2012, the WEP had 414 corporate signatories from around the world.¹⁹ Of these, 29 signatories work in the ICT industry.

One of the WEP principles is to establish a zero-tolerance policy towards all forms of violence at work, including verbal and/or physical abuse and to prevent sexual harassment. This principle brings the issue of VAW with internet intermediaries to the fore, and provides an opening for discussing gender issues related user-rights, content regulation, and VAW monitoring.

The *15 Years Review of the United Nations Special Rapporteur on Violence Against Women, its Causes and Consequences* (UN SRVAW) notes how the mandate has addressed accountability of transnational corporations who operate across states and whose actions sometimes adversely affect women as follows:

The SRVAW recommended gender impact studies, inclusion of gender as part of corporate responsibility, and the institutionalization of codes of conduct incorporating human rights within corporations or as part of social responsibility of corporations, rather than complete reliance upon State conditionality—for that is contingent upon not just a strong State, but one that is also committed to women's human rights.²⁰

6.4. Existing responses and interventions

Internet intermediaries – particularly social networking platforms – have voluntarily recognised that certain behaviours cannot and should not be tolerated online. For example, Facebook, Twitter and YouTube, all have policies on the "Terms of Use" and "Community Standards" that bar hate speech and abuse. All three platforms have online mechanisms by which to report and/or flag abuse.

Nevertheless, these mechanisms can be abused and inadvertently facilitate online harassment and violations against women. Differential standards are also applied to what content is taken down and what content is allowed to remain online.

For example, "Women say they have been banned from Facebook and seen their pages removed for posting images of cupcakes iced like labia, pictures of breastfeeding mothers and photographs of women post-mastectomy."²¹ In contrast, it took a massive public outcry and a Change.org petition garnering over 200,000 signatures for Facebook to even begin responding to the issue of the hundreds of pages on the

¹⁷ UN News. (2010, 18 November). Secretary-General, in message, spotlights role of business in ending violence against women by embracing corporate social responsibility principles. <http://www.un.org/News/Press/docs/2010/sgsm13257.doc.htm>

¹⁸ See the official website of UN Women's "Women's Empowerment Principles" for more details on each specific principle and recommended practices: <http://www.wepinciples.org/Site/PrincipleOverview>

¹⁹ Women's Empowerment Principles Signatories as of 17 April 2012, available at: http://www.unglobalcompact.org/docs/issues_doc/human_rights/WEPs_CEO_Statement_of_Support_Signatories.pdf

²⁰ UN SRVAW. (2009). *15 Years of the United Nations Special Rapporteur on Violence against women, its Causes and Consequences*. UN OHCHR. <http://www.ohchr.org/Documents/Issues/Women/15YearReviewofVAWMandate.pdf>

network which offer a barrage of vitriolic hate speech against women, photos of women's bloodied and beaten bodies, jokes promoting the use of drugs to rape women, and more. Feminist activist Soraya Chemly has pointed out, "Facebook clearly accepts representations of some forms of violence - namely violence against women - as qualitatively different from others."²²

Defining "hate speech", "abuse" and "incitement to violence" as outlined in corporate policies is far from straightforward; it involves a constant process of interpretation, and interpretation of these policies often results in the allowance of content promoting violence against women, while deliberately censoring women's autonomy and their exercise of free speech online.

Consider Dana Bakdounes, a Syrian woman and member of the Uprising of Women in the Arab World Facebook group, which had its administrators suspended after photographs of an un-veiled Bakdounes were posted on its site.²³ The suspension was triggered by a tide of reports of offensive content - undoubtedly sent by those who protested Bakdounes' right to be pictured without a hijab. These protests, and Facebook's decision to suspend the group, essentially silenced women's rights to freedom of expression, freedom of assembly, and freedom of religion and belief.

Feminist blogger Anita Sarkeesian hosts a video blog dissecting misogyny and sexism in mainstream popular culture. After starting a Kickstarter campaign to obtain funding for a new research project on the misogynistic portrayal of women in video games, she was the subject of online stalking, threats, harassment, and privacy violations. An interactive online game was created inviting users to "Beat Up Anita Sarkeesian" by clicking on an image of her face, which became increasingly bloodied and bruised with each click. To add insult to injury, the output of her own feminist research, a video post entitled "Damsel in Distress: Part II, Trope vs. Women in Video Games", was taken down by YouTube for "violating" the Terms of Service after being flagged an inordinate number of times by those seeking to silence her.

Sarkeesian appealed the decision, and the video was eventually reinstated.²⁴ YouTube attributed the decision to "human error" and highlighted its appeals process²⁵ as an important mechanism in providing redress, but the question remains as to why the video was removed in the first place. In a phone interview, "a YouTube spokesperson explained that all YouTube content is screened by their staff, though not always immediately after the videos are posted, and that while a high number of flags can cause a video to move up the list for review, flags alone can't get a video pulled."²⁶ Once again, the policies aimed to protect users from being subjected to inappropriate content were implemented in a way to further silence a victim/survivor of technology-related VAW. This speaks to an urgent need to look behind the mere existence of policies, to the mores and practices around their interpretation and implementation, and the role of bystanders in digital space.

²¹ Bates, L. (2013, 19 February). Does Facebook have a problem with women? *The Guardian*. <http://www.theguardian.com/lifeandstyle/2013/feb/19/facebook-images-rape-domestic-violence>

²² Ibid.

²³ Anderson, S. (2012, 14 November). Why did Facebook censor this picture? *Foreign Policy Blog*. http://blog.foreignpolicy.com/posts/2012/11/14/why_did_facebook_censor_this_photograph

²⁴ See: <https://twitter.com/femfreq/status/339506260867170304>

²⁵ <https://support.google.com/youtube/answer/185111?hl=en>

²⁶ Hamilton, K. (2013, 28 May). New Anita Sarkeesian video calls out gaming's 'women in refrigerators'. *Kotaku*. <http://kotaku.com/heres-anita-sarkeesians-second-tropes-vs-women-in-g-510123131>

Writing for GenderIT.org, Carly Nyst highlights:²⁷

A number of key gendered norms and assumptions have informed, and thus restrained, the approach of internet intermediaries to gender-based violence online:

1. Speech that trivialises or glorifies violence against women does not amount to hate speech

In response to the #Fbrape campaign by Women, Action and The Media against the targeting of women with images and content that threaten or incite gender-based hate, Facebook argued that, while the platform does not permit “hate speech”, there are instances of offensive content, including distasteful humour, that do not constitute “hate speech”, and thus do not justify immediate removal. Facebook’s statement went on to equate gender-based hate speech with “insensitive or cruel content”, revealing a fundamental misapprehension of the destructive and threatening nature of gender-based hate speech. Such speech must be seen in the context of historical and institutionalised violence and discrimination against women, and the monumental power differential that persists between men and women. Equating gender-based hatred with insulting remarks only further undermines the position of women.

2. Harassment online does not amount to violence unless there is the probability of “imminent harm” or “real violence”

This misconception clearly factors into the risk analysis of internet intermediaries when judging their approach to gender-based hatred and harassment. It reveals a lack of understanding of inappropriateness of concepts such as “imminent” or “genuine” for women who experience rape and domestic violence as pervasive threats. It also fails to consider the very real effects of violent and sustained harassment, including anxiety and changes in behaviour. Such an attitude is clear in the lack of response by Twitter to the various instances of rape and death threats received by prominent feminist activists throughout 2013. Were such threats made by other means they would be viewed as indicative of very real and imminent harm and would be immediately reported to police, yet when made on Twitter they were diminished.

3. Common misogynistic slurs do not present a real threat of violence

There is a clear perception on the part of internet intermediaries that the use of common misogynistic slurs such as “bitch”, “slut”, “whore”, etc. have reached such frequency in the mainstream media that their employment as a means of harassment or discrimination online is acceptable in all circumstances. Facebook’s response to the online hatred directed at

²⁷ Nyst, C. (2013, 26 November). Internet intermediaries and violence against women – how gender-based harassment falls through the digital cracks. *GenderIT.org*. <http://www.genderit.org/feminist-talk/how-gender-based-harassment-falls-through-digital-cracks>

Icelandic woman Thorlaug Agustsdottir revealed the problematic attitude of the site to hate speech: “It is very important to point out that what one person finds offensive another can find entertaining – just as telling a rude joke won’t get you thrown out of your local pub, it won’t get you thrown off Facebook.”

4. Online reporting mechanisms are deemed sufficient to ensure that gender-based hate speech is brought to light

In the aftermath of recent rape threats and bomb threats distributed via Twitter, the platform announced the introduction of an In-Tweet report button, with which users can report behaviour directly from a tweet. However, no moderation is instituted, meaning that if offensive or violent tweets go unreported – because the recipient fears reprisals, for example – then no action will be taken, unless others are willing to act on her behalf.

Areas for further research and advocacy: The gendered norms and assumptions underlying internet intermediaries’ responses point to the necessity of increased awareness raising, dialogue, and gender-sensitivity training with internet intermediaries, particularly the staff of the user-policy formation and monitoring departments; in addition to continued public activism and campaigning at the national and transnational levels. Research needs to explore how intermediaries work with law enforcement when technology-related violence extends offline, especially for users who live outside the countries where these corporations have operating offices. Internet intermediaries, and particularly transnational corporations such as Google and Facebook with over one billion registered users each, need to be accountable for the ways in which they infringe on the rights of women users’ and facilitate technology-related VAW through the application of their policies and practices, and their responsibility to act and prevent such violations from occurring.

Designing the research: The above discussions constitute the background and theoretical framework for undertaking a research project that documents women and girls’ experiences of technology-related VAW and their attempts to access justice, analysing the adequacy and effectiveness of legal remedies and corporate redress mechanisms in different country contexts. The research design—the goals, objectives, research questions, and activities—are explained in specific detail in the following section.

7. Works cited

- Anderson, S. (2012, 14 November). Why did Facebook censor this picture?. *Foreign Policy Blog*. http://blog.foreignpolicy.com/posts/2012/11/14/why_did_facebook_censor_this_photograph
- Association for Progressive Communications. (2011). “Statement to the 57th Session of the CSW: Violence against women and information and communications technology.” <https://www.apc.org/en/system/files/CSW%20APC%20statement%20FINAL%20VERSION.pdf>
- Bates, L. (2013, 19 February). Does Facebook have a problem with women? *The Guardian*. <http://www.theguardian.com/lifeandstyle/2013/feb/19/facebook-images-rape-domestic-violence>
- Comninos, A. (2012). *The liability of internet intermediaries in Nigeria, Kenya, South Africa and Uganda: An uncertain terrain*. Association for Progressive Communications. <http://www.apc.org/en/node/15649>

- Fialova, K., & Fascendini, F. (2011). *Voices from Digital Spaces: Technology related violence against women*. Association for Progressive Communications. <http://www.genderit.org/node/3539>
- Gurusurthy, A., & Menon, M. (2009, 3 October). Violence against Women via Cyberspace. *Economic & Political Weekly (EPW)*, XLIV(4).
- Hamilton, K. (2013, 28 May). New Anita Sarkeesian video calls out gaming's 'women in refrigerators'. *Kotaku*. <http://kotaku.com/heres-anita-sarkeesians-second-tropes-vs-women-in-g-510123131>
- Nyst, C. (2013, 26 November). Internet intermediaries and violence against women – towards intermediary responsibility. *GenderIT.org*. <http://www.genderit.org/feminist-talk/towards-internet-intermediary-responsibility>
- Nyst, C. (2013, 26 November). Internet intermediaries and violence against women – how gender-based harassment falls through the digital cracks. *GenderIT.org*. <http://www.genderit.org/feminist-talk/how-gender-based-harassment-falls-through-digital-cracks>
- Powell, A. (2009). *New technologies, unauthorised visual images and sexual assault*. Australian Institute of Family Studies. www.aifs.gov.au/acssa/pubs/newsletter/n23pdf/n23c.pdf
- UN News. (2010, 18 November). Secretary-General, in message, spotlights role of business in ending violence against women by embracing corporate social responsibility principles. *New York Department of Public Information*. <http://www.un.org/News/Press/docs/2010/sgsm13257.doc.htm>
- UN OHCHR. (2011). *Guiding Principles on Business and Human Rights: Implementing the “Protect, Respect and Remedy” Framework*. http://www.ohchr.org/Documents/Publications/GuidingPrinciplesBusinessHR_EN.pdf
- UN Secretary General. (2006). In-depth Study on All Forms of Violence Against Women (A/61/122/Add.1/Corr.1). <http://daccess-dds-ny.un.org/doc/UNDOC/GEN/N06/419/74/PDF/N0641974.pdf?OpenElement>
- UN SRSG on Human Rights, Transnational Corporations and Other Business Enterprises. (2009). *Integrating a Gender Perspective into the UN ‘Protect, Respect and Remedy’ Framework: Consultation Summary*. <http://www.reports-and-materials.org/Gender-meeting-for-Ruggie-29-Jun-2009.pdf>
- UN SRVAW. (2009). *15 Years of the United Nations Special Rapporteur on Violence against women, its Causes and Consequences*. <http://www.ohchr.org/Documents/Issues/Women/15YearReviewofVAWMandate.pdf>
- UN Women & UN Global Compact. (2012). CEO Statement of Support and List of Signatories. http://www.unglobalcompact.org/docs/issues_doc/human_rights/WEPS_CEO_Statement_of_Support_Signatories.pdf
- UN Women. Women’s Empowerment Principles <http://www.weprinciples.org/Site/PrincipleOverview>
- Women’s Legal and Human Rights Bureau (WLB). (n/d). Study on ICT, VAW and Sexuality: A Policy Advocacy. (Unpublished paper). Manila: Women’s Legal and Human Rights Bureau.
- Women’s Legal and Human Rights Bureau. (2010). *Understanding Women’s Access to Justice*. <http://www.ohchr.org/Documents/HRBodies/CEDAW/AccessToJustice/WomensLegalAndHumanRightsBureau.pdf>

- Women's Legal and Human Rights Bureau. (2010). *Women's Access to Justice: Mapping of Domestic Legal Remedies on Violence Against Women*. Manila: Women's Legal and Human Rights Bureau.

II. Research design

1. Research as an output of the FLOW/EndVAW project

This research is being undertaken as part of APC's overarching multi-year programme "End violence: Women's rights and safety online" (EndVAW), supported by the Dutch Ministry of Foreign Affairs' Funding Leadership Opportunities for Women (FLOW) initiative.

The proposed research relates to Outcomes 2 and 3 of the FLOW/End Violence project:

- FLOW Outcome 2: Remedies and policies that address technology-related VAW are developed through research and advocacy by women leaders and women's rights organisations.
- FLOW Outcome 3: Women leaders are effectively engaging private sector (social networking, web hosting companies and mobile phone companies), in partnership with other expert NGOs to develop company user policies that protect the safety and security of women's rights.

Within these two Outcomes, the following key outputs are expected from the research:

- Output 2.1.1: Multi-country "Case Study" research design, involving the identification of cases in seven countries and research instruments that provide for comparative analysis.
- Output 2.1.2: Up to 25 quality case studies identified in seven countries that provide insights into legal remedies.
- Output 3.1: Study on corporate user policies that provide for the protection of women's rights, including safety and security of users.
- Output 3.1.1: Corporate policy study to provide comparative information on at least seven countries, plus a global study of a major social networking corporation.
- Output 3.1.2: Interest and participation from up to 10 key private sector actors in the study (either participating in research design, providing information as informants, and providing critical feedback about the research).

2. Research goals

The overarching goals of the research are to:

1. *Gather evidence to increase our understanding of the dynamics of technology-related VAW, and of what works and what doesn't in the fight against these forms of violence.*
2. *Develop recommendations for effective evidence-based legal, civic and community based response strategies that can be readily adopted by key stakeholders (mainly, women, women advocates, public officials, legal professionals, and corporate agents) to fight technology-related VAW.*
3. *Disseminate information that helps women and girls who fall victim of technology-related violence, know what to do to stop the abuse, realise what charges they can report and to whom, and become aware of the kind of help they can get.*

3. Case study methodology and corresponding activities

Case studies as a methodology are particularly apt for research when a complex phenomena needs to be explored more in-depth. Case studies showcase the perspectives and experiences of those most directly affected by a phenomena – in this case, women’s experiences of technology-related VAW. An important strength of case studies is that they encourage triangulation of data; that is, they employ multiple research methods in sourcing and collecting data, in order to strengthen the validity of the research findings.

This study involves the collection of case studies that examine in-depth women’s experiences of technology-related VAW, their attempts to access justice; and the corresponding *availability and effectiveness of existing legal remedies and corporate redress mechanisms for victims/survivors*. It will gather data across seven countries as well as at the international level, through a combination of desk-review, interviewing, and focus groups discussions. It prioritises the collection of qualitative data about challenges to/opportunities for legal and civic remedies, but also seeks to bring in quantitative data on the prevalence of technology-related VAW.

Primary research activities:

1. **Examination of domestic legal remedies, through desk review and interviews.** This entails identifying what constitutes harm brought about by technology-related VAW as recognised in different domestic laws, and the processes, mechanisms, and institutions involved in providing remedies and affording women’s access to justice.

This includes examining the existence of laws addressing a particular harm/violation, the enforcement of said laws through investigation and prosecution, and the trial of the same through judicial processes. It likewise examines relief provided by the state; state laws, policy frameworks and justice mechanisms maintained or operated by the state and its agents; and other mechanisms where state authority is directly involved either in national human rights institutions, gender and women commission, or ICT and telecommunication commission.

2. **Interviewing and documenting experiences of women victims/survivors of technology-related VAW**, to bring out their voices and show how they exercise and negotiate their agency in different contexts when seeking remedy.
3. **Mapping of the internet intermediaries’ policies and practices** at the domestic level to protect users’ rights and provide redress when violations have occurred.²⁸
This includes desk review and the conducting of interviews with corporate representatives to identify and analyse:

- a) Which rights violations are explicitly recognised and provided for in corporate policies
- b) The processes for reporting violations
- c) The support mechanisms in place for victims/survivors

²⁸ We recognise that data collection is surely needed on prevention strategies by internet intermediaries, but this lies beyond the scope of this research, which as a first step is seeking to map out the options for recourse that victims/survivors have to help ensure/improve women’s access to justice.

- d) The extent to which internet intermediaries collaborate with other institutions (e.g., police, social service orgs, judiciary, national commissions, etc.) to facilitate victims/survivors' access to justice
- e) How intermediaries' policies are developed and reviewed and whether a consultative process is followed; and how the internal structure impacts the effectiveness of policy implementation to improve women's access to justice in cases of technology-related VAW.

4. Surveys to collect information on technology-related VAW in the study countries.

Underreporting of VAW remains a universal barrier to developing effective counter-measures, and even more so with technology-related VAW which is not yet widely recognised. The survey will take APC's existing mapping tool as a point of departure. This tool provides a framework for categorising the forms, manifestations, impacts and perpetrators of technology-related VAW. Surveys focused on the study countries will be conducted to help expand information on (a) technology-related VAW, (b) the characteristics of VAW that occurs through the major platforms (e.g., Twitter, mobile phones, Facebook), and by extension (c) which internet intermediaries should be strategic allies in providing redress and developing best practices against VAW.

- 5. **Desk review on new and emerging laws and corporate policies at the international level** that will shed light on best practices and help shape policy recommendations arising from the national-level research. This will include reviews of two transnational platforms, Facebook and Google's YouTube.

Access to justice²⁹

This research draws from the Women's Legal and Human Rights Bureau's "Access to Justice" framework, which will examine the strengths and limitations of: (1) laws on VAW and ICT; (2) existing policy frameworks; and (3) available complaint mechanisms in relation to women's agency and capacity to seek domestic remedy. This framework sees the need to look beyond legal measures and into the interplay of politics, economics and culture in women's access to justice in cases of violence. The existence of domestic legal remedies and multi-disciplinary support services alone cannot be made to measure women's access to justice when the circumstances of access are affected by factors not only inside the legal system, but also outside it. Access to justice looks at development of women as a whole; it sees women as active agents, and in best position to identify their own strengths and needs. Indicators for domestic legal remedies and corporate policies/redress mechanisms are discussed in more detail below.

Developing the case studies

National level case studies will use a combination of the aforementioned desk review and interviewing techniques to gather and report the following information for each case:

1. The perspective and experience of the Victim/Survivor (based on desk review and/or in-depth interview with victim/survivor)

²⁹ The Access to Justice Framework elaborated here comes from the Women's Legal and Human Rights Bureau's research on *Women's Access to Justice: Mapping of Domestic Legal Remedies on Violence Against Women* (2010). See as well: WLB, "Understanding women's access to justice", available at: <http://www.ohchr.org/Documents/HRBodies/CEDAW/AccessToJustice/WomensLegalAndHumanRightsBureau.pdf>

- o Her profile
 - o The violations she experienced
 - o How this impacted her
 - o The help she felt she needed
 - o The obstacles she faced getting the help she needed
 - o The strategies she used to seek help
 - o The help she got and the remedy she was able to access.
2. How national-level laws facilitate or hinder access to justice (based primarily on study country desk review, but verified through conversation with victim/survivor)
 - o Which national laws can be used to provide remedy
 - o What gaps exist in national laws.
 3. How those responsible for the implementation of laws facilitate or hinder access to justice (based on desk review and interviews with members of law enforcement and victim, as pertinent)
 - o Whether law enforcement officials (police, lawyers, judges) effectively implement national laws
 - o How attitudes, training and capacity of these stakeholders affects implementation of national laws.
 4. In cases where internet intermediaries (social networking services, webhosting companies, or mobile phone companies) are implicated, how their policies and redress mechanisms facilitate/obstruct her access to justice (based on desk review and interviews with corporate representatives and victim/survivor)
 - o Do corporate policies provide protection for women victims/survivors of technology-related VAW?
 - o Do corporate practices and procedures ensure effective implementation of avowed policies?
 5. Concluding remarks that tie together above details of the case in regards to recommendations for improvement in laws and policy to ensure access to justice.

Note: Each country partner will develop three to four in-depth case studies, providing a total of 21 to 28 case studies in the overall research as outlined for FLOW Outcome 2.

For each country partner, only one to two of the case studies will necessarily include the fourth element on internet intermediaries. One case should involve a national-level actor (i.e. mobile phone company or ISP), and one case should involve a transnational actor (Facebook, Twitter, Google, etc.). This will result in 7-14 case studies that will feed into the research requirements of FLOW Outcome 3. The rest of FLOW Outcome 3 will be addressed by the literature review and interviews conducted at the international level.

4. Criteria for selecting cases

The selected cases in this research were specifically/purposively varied in order to tap into the different experiences of women from different countries and contexts. In the selection of the cases, the following general guidelines were followed:

1. The case must have involved technology-related violence against women.
 - 1.1. VAW as defined in the UN Declaration on the Elimination of Violence against Women (DEVAW) which states that violence against women means “any act of gender-based violence that results in, or is likely to result in, physical, sexual or psychological harm or suffering to women, including threats of such acts, coercion or arbitrary deprivation of liberty, whether occurring in public or in private life.” We take this definition to include anyone who self-identifies as a woman, including intersex, transgender and transsexual women.
 - 1.2. Technology-related VAW is VAW that must have been committed through the use of ICT and perpetrated by an individual or private company. The research will not include cases wherein technology-related VAW is committed by the state or syndicated group.
 - 1.3. The case should be selected on the prevalence of this particular type of technology-related VAW that takes place within the country (representative cases) OR the country partner has particular interest in pursuing this particular type of VAW in regards to their advocacy activities (key cases).
2. The woman must have attempted to access justice, it not being necessary that the case be fully adjudicated on its merits or have reached the highest tribunal of the land; it suffices that the case shows the effort exerted by the woman-survivor to seek domestic remedy for the grievance in the best possible ways and means available to her. This may involve the most basic such as the filing of complaints with relevant authorities such as the police, service providers, or with internet intermediaries to more advanced actions such as the filing of cases in courts or appealing decisions with higher courts.
 - 2.1. In the selection of cases, priority shall be given to those that have undergone enforcement and judicial processes namely investigation, prosecution and trial of the case; and those recommended by women’s groups as indicative of a woman’s struggle to access justice in the country’s formal legal system.
 - 2.2. Depending on the country’s context, a case wherein there is no existing domestic remedy available to the woman victim/survivor of technology-related VAW but the woman on her own acted on the violation she experienced.
 - 2.3. The woman survivor must be available for an in-depth interview and be willing and able to share and document her experience of accessing justice in cases of violence or someone who has personal knowledge of the case. The person/s gathering and analysing the data shall exercise utmost care to ensure privacy and protection of the identity of the victim/survivor.
3. In the selection of cases, at least two are where internet intermediaries (social networking services, mobile phone company, web host, telecommunication company) are implicated. Cases should ideally involve different intermediaries – for example, one may be a transnational corporation, and one may be a national-level actor. Selection can be based on the popularity of particular social networking platforms/mobile phone companies/web hosts at the national level.

4. Intersectionality in terms of identities/demographics of survivors is also prioritised in the overall selection of the cases, to enable us to look at a diversity of women affected. For example, exploring cases involving women of diverse economic classes, ethnic and racial backgrounds, ages, sexual orientation, ability, etc.

5. Indicators for analysis

In relation to domestic legal remedies, effectiveness can be indicated by the presence of the following elements of access to justice:

a. Participation and critical engagement

Violence against women perpetuated through ICT calls and necessitates an empowerment approach to tackle it. Women are not simply static victims. One has to look into different situations of women in different contexts and see how they exercise and negotiate their agency in said contexts. We have to acknowledge that women react, respond and can choose to respond by empowering themselves. The approach to address technology-related VAW must not be merely “protectionist” but empowering by letting women speak for themselves.

This element calls for the critical visibility and participation of women-survivors in making decisions regarding the grievance she experienced as well as her decision to pursue and seek justice for the same. Necessarily part of participation and critical engagement of women is her awareness, first and foremost of her rights, the remedies available to her, the institutions involved and the procedures she has to follow.

b. Adequacy

As generally recognised in the studies of technology-related VAW, the difficulty in addressing the problem lies largely in applying existing norms to a technology that did not exist when laws and policies were drafted. There are available substantive laws which can be invoked or explored in cases of technology-related VAW which can be found in the penal codes, VAW and sexual violence laws and technology-related laws. Still, the adequacy of available remedy for cases of technology-related VAW remains a question.

Adequacy as an element of access to justice covers a) the existence of legal and other possible remedies in cases of violence against women; b) the availability of the remedies; and c) their affordability.

c. Effectiveness

The element of effectiveness necessarily presupposes that an adequate system (characterised by existence of remedies, availability, and affordability) already exists and addresses the distinct characteristics of technology-related VAW. Competent, impartial, independent and gender-sensitive legal system and duty bearers and women’s active participation in the process are parts and parcels of effectiveness. In addition, it pertains to the effective, speedy and immediate enforcement of the fruits of the processes, and the enjoyment of the same by the woman-survivor. It also includes the existence of immediate protective measures and the existence of monitoring oversight on the part of state actors to further facilitate and improve women’s access to justice.

d. Legitimacy

This element focuses on the transparency, accountability, and credibility of the legal system and the duty bearers and to the political will of the State to address violence against women.

e. Changes in attitudes

This element is two tiered: first, it looks into how a particular woman's case and the collective support thereof by women's groups changes the practices and attitudes of the duty bearers and the legal system in general, and second, how the same case, affects the collective practice and attitude of women's organisation, leading them to lobby before the state in the formulation of laws and policies more responsive to the experiences and needs of women.

f. Enabling environment for access to justice

The manifestations of VAW depend on the specific social, economic, cultural and political context. New forms of VAW may arise when societies undergo demographic, political, economic, and cultural or say technological shifts/changes such as when ICT enters the scene. The context per country may vary depending on how the particular government perceives VAW, including those acts carried out through the use of ICT, and how the legal framework views women and women's rights in their respective countries.

In relation to corporate policies/redress mechanisms, indicators also draw from the above elements of Access to Justice, as well as concepts of gender-mainstreaming best practices.

A holistic approach is needed to ending technology-related VAW, of which a key part is increased prevention efforts. However, for the purposes of this research we seek to map out what options victims/survivors have available to them *after violations have occurred*.

Therefore, key to our analysis is whether or not there exists recognition that a violation is a form of VAW (and as such a violation of women's rights) in corporate policies, so that when it happens, survivors have access to redress.

Recognition has two aspects: first there is the impact of ICT on VAW, in terms of recognising *the harm* (looking at the ways its done and how and where), and examining *the range of rights* that are being violated. Second, the need to recognise that there is a gendered dimension to internet use and governance, in terms of access; norms and discourses; ownership and decision-making; and unequal power relations.

Combining this approach with the Access to Justice framework, the following indicators can be used to assess corporate policies and practices. Note, not all of these will necessarily be addressed in analysis. They provide a framework to help guide data collection and interviews:

Adequacy

- Existence of corporate policies explicitly preventing and sanctioning hate-speech and abuse on the basis of race, ethnicity, national origin, religion, sex, gender, sexual orientation, disability or medical condition.
- Appropriateness of these policies, so that they are in line with what the national law says in terms of protecting against VAW.
- Women who have experienced technology-related VAW can easily access to corporate mechanisms.

- Simple reporting procedure (e.g. automated reporting system, accessible via phone/internet, no cost to person reporting).
- Existence of specific department to deal with reports/complaints promptly, and enough staff for the volume of complaints.
- Policies outline when/how they will collaborate with police/law enforcement, and a mechanism in place in cases of technology-related VAW.

Effectiveness

- The redress mechanism ensures an immediate end to harassment/stalking/privacy violations through the medium reported (i.e. blocking contact (messages/texts/calls) from the harasser, removing inflammatory material, deleting posts).
- Appropriate gender-sensitive indicators for monitoring reports of VAW have been developed, and are being reported on.
- Statistical systems and project-monitoring systems that provide gender-disaggregated data are being maintained.
- Gender equity is addressed in all training and staff development initiatives, particularly for those responding to complaints.

Women's critical engagement (*specifically in relation to decision-making and policy formation, as well as monitoring and addressing rights violations*)

- Women's rights advocates and gender-experts are represented in policy-formation.
- Women's rights advocates and gender-experts are present in corporate decision-making bodies.
- Partnerships with local women's nongovernmental organisations (NGOs), grassroots organisations, research centres, (etc.) for data collection, analysis and policy change exist or are being explored.

Legitimacy

- Procedures and actions for monitoring of rights violations are transparent (i.e. existence of data, gender-disaggregated, willingness to share)
- Where content monitoring is conducted by third party/external entity, mechanisms to ensure accountability are in place.

Enabling environment

- National legislative framework addresses VAW as a source of guidance for corporate policies.
- Civil or criminal legal remedies address harassment, hate speech, and incitement to violence.
- Corporations are signatory to international commitments regarding human rights, women's empowerment, etc.
- Funds are being allocated for gender-capacity-building.

6. Overarching research matrix

The following matrix summarises the key objectives, research questions and methods for the research.

Goals	Objectives	Research questions	Methods	Notes
1. Gather evidence to increase our understanding of the dynamics of technology-related VAW	1.1. To surface the voices/ experiences of victims/ survivors in seeking remedy in cases of technology-related VAW and to identify insights from their experiences.	-How did the experience impact the survivor? -How did the woman access the remedy available to her? -How did the woman make decisions about the available options presented to her given her capacity and context? -What were the factors that limit or facilitate her decision to seek a particular remedy?	Developing case studies involving desk research and in-depth interviews with victims/survivors where possible	Based on FLOW proposal, country partners will conduct 3-4 case studies each.
	1.2. To identify existing corporate policies that internet intermediaries have in place and to surface the gaps and limitations of these policies in relation to stopping technology-related VAW	-What internal policies (codes of conduct/terms of use, content regulation, privacy, complaints) do selected internet intermediaries have in place to protect users' rights? -How can these policies be used to protect women's rights? -Do these policies support, fall short of, or go beyond protection provided for women by national level laws?	Desk review to map existing corporate policies and analysis through access to justice-based indicators.	Each partner will develop 3-4 case studies overall, out of which two should implicate internet intermediaries. One should be a national-level social networking service, web hosting company, or mobile phone provider. It will be this national-level intermediary's policies that partners map through desk review. The second case should implicate a transnational actor (Facebook, Google, Twitter, etc.), whose policies will be mapped by the international level research.

Goals	Objectives	Research questions	Methods	Notes
	1.3. To gather quantitative data on the prevalence of technology-related VAW	<p>-How is technology being used to perpetrate violence against women?</p> <p>-What technologies/ platforms are most commonly implicated?</p> <p>-What are the demographics of women/girls being affected?</p>	Quantitative analysis of data concerning VAW online collected using APC's online mapping tool ³⁰	This is not intended as the main method of data gathering for the research. It is intended primarily as a quantitative overview of the cases reported, with some qualitative illustration. Data gathered will support research findings from the main methods of in-depth interviews and desk review.
2. Develop recommendations for effective evidence-based legal, civic and community and non-legal response strategies that can be readily adopted by key stakeholders (mainly, women, women's advocates, public officials, legal professionals and corporate agents) to fight technology-related VAW	2.1. To identify available domestic legal remedy in cases of technology-related VAW and surface the gaps and limitations of said remedies.	<p>-What are the available substantive and procedural laws in cases of technology-related VAW, including the respective procedures and the institutions involved, which refers to justice mechanisms maintained or operated by the state and its agents; and other mechanisms where state authority is directly involved either in their creation, constitution, composition or accountability?</p> <p>-What particular harm/violation/technology-related VAW do these laws address?</p> <p>-How do these laws view women and violence against women in particular technology-related VAW?</p> <p>-How does the available legal remedy address the challenge posed by the distinct characteristics of technology-related VAW?</p>	<p>a) Desk review to map available legal remedies (reviewing APC research, country baseline studies and other relevant research)</p> <p>b) Interviews with law enforcement and social service providers (NGOs).</p>	This includes bringing a critical feminist analysis to laws and remedies in our analysis; identifying which laws may contribute to paternalistic protectionism and censorship that actually limits women's and marginalised communities' rights (e.g. may criminalise sexuality, infringe on freedom of expression, actually limit women's critical participation and freedom of assembly in online spaces, etc.).

³⁰<https://www.takebackthetech.net/mapit>

Goals	Objectives	Research questions	Methods	Notes
		-What are the other available remedies and how do they connect/mesh with domestic legal remedy?		
	2.2. To identify and analyse the adequacy/ effectiveness of corporate policy implementation and redress mechanisms, as well as highlight gaps in current practices	-What redress mechanisms exist in relation to technology-related VAW? -How are complaints/reports of online VAW received and addressed by internet intermediaries? -How do internal practices enable/prevent access to justice for victims/survivors of technology-related VAW?	Interviews with internet intermediaries representatives and analysis based on access to justice based indicators	Interview will be with the same national-level intermediary selected above (Objective 2.2). Interviews at the international level will be conducted with representatives of two transnational social networking services, depending on which ones are most relevant to national level advocacy (by research consultant).
3. Disseminate information that helps women and girls who fall victim to technology-related violence know what to do to stop the abuse, realise what charges they can report and to whom, and become aware of the kind of help they can get	3.1. To forward recommendations for ICT/VAW policy based on women's experiences in seeking domestic remedy in cases of technology-related VAW	-How will this research help in strengthening women's capacity in responding to technology-related VAW? -How will the research strengthen the advocacy to end violence against women? -How will the research improve and facilitate access to justice for women victims/survivors of technology-related VAW and VAW in general?	Inviting feedback from relevant stakeholders (women's rights advocates, internet rights advocates, online child safety advocates, internet intermediary representatives, etc.) on the research findings	This activity relates to the advocacy efforts after the research results have been analysed and reported on (expected to happen in Phase II between June and December 2014).

7. Ethics in the research process

This study falls into the category of research on violence against women (VAW) and fits clearly within the realm of sensitive research topic. Our research on domestic legal remedies specifically involves women across seven countries sharing their experiences of victimisation and survival, and they could be speaking out in a societal context of disbelief, fear and shame. This research hopes to give women and girls who

have experienced violence and rights violations through the opportunity to be heard and to contribute to the improvement of their lives through appropriate policy and legislation. The research shall elicit and analyse knowledge in a way that can be used by women to alter oppressive and exploitative conditions in society.

APC's prior research has begun to show that technology-related VAW is not isolated, but often connects to existing and readily recognised forms of VAW – particularly intimate partner violence, sexual violence, and domestic violence. Taking this as a starting point, this research seeks to follow the guiding principles to conducting domestic violence research, as laid out by the World Health Organization in their 2001 report *Putting Women First: Ethical and Safety Recommendations for Research on Domestic Violence against Women*.

The physical safety of respondents and interviewers from potential retaliatory violence by the perpetrator or perpetrators is of prime importance. Even where respondents do not appear to be in situations that pose extended threats to security and safety, having such protocols in place helps teams to assess as fully as possible the possible risks and to respond appropriately.

WHO Guiding Principles for Domestic Violence Research

- a. The safety of respondents and the research team is paramount, and should guide all project decisions.
- b. Prevalence studies need to be methodologically sound and to build upon current research experience about how to minimise the under-reporting of violence.
- c. Protecting confidentiality is essential to ensure both women's safety and data quality.
- d. All research team members should be carefully selected and receive specialised training and ongoing support.
- e. The study design must include actions aimed at reducing any possible distress caused to the participants by the research.
- f. Fieldworkers should be trained to refer women requesting assistance to available local services and sources of support. Where few resources exist, it may be necessary for the study to create short-term support mechanisms.
- g. Researchers and donors have an ethical obligation to help ensure that their findings are properly interpreted and used to advance policy and intervention development.
- h. Violence questions should only be incorporated into surveys designed for other purposes when ethical and methodological requirements can be met.

The following section lays out in more detail the ethical concerns and guiding protocols for the research.³¹ Ethical concerns focus on respect for persons, justice and fairness. Security concerns are integrated within each section.

³¹ In some instances these have been reproduced verbatim from the original WHO report, available in English, French and Spanish here: http://www.who.int/gender/documents/violence/who_fch_gwh_01.1/en

A. Collaboration and partnership amongst partners

The principles of collaborative partnership shall guide the research. Collaboration is important in building feminist-informed knowledge and projects.

- In collaborative partnership, the responsibilities of research partners are clear which allows the sharing of mutual capacity building and sharing of comparative strengths. It also entails acknowledging limitations and weaknesses as researchers.
- Deep collaboration in research conceptualisation and design means that research goals, questions and methods are open for negotiation and discussion. It shall be ensure that parties involve put significant effort in the process and mutually benefit.
- The research design and process shall be informed by the different contextual realities of researchers such as researchers are conscious of their situatedness, perspective when interacting with others and the power dynamics they may bring in. Geopolitical differences, differences in schedule, skills and resources can affect ways of working.
- Issues and potential hierarchies that may arise from these differences shall be dealt through an open and clear communication. Research partners shall confront the issues directly, respectfully and together.
- Keeping up with the principles of collaboration, co-authorship shall be employed. There shall also be clear articulation of other recognition associated with research.

B. The relationship of participants and researchers

1. Obtaining informed consent

- Participants in the research are treated as human beings with agency – capable of determining and deciding what is best for them and not mere subjects or as means to extract data.
- As with respect to their self-determination, a) the nature of the research, b) any risks and benefits which might result from their participation, c) their rights to refuse to participate or to end their participation without penalty, and d) the means by which they can contact the researcher shall be first explained to potential research participants in a language they understand.
- It is imperative to stress that consent is voluntary, and as such can be withdrawn at any time prior to the publication of research outputs. Researchers must ensure the possibility for participants to withdraw their consent (at minimum by providing a way to contact field researchers).
- Only those who express willingness shall be considered for the study.

2. Providing support to participants

Research participants stand to face positive as well as negative effects from their involvement/ participation in the research. The researcher shall ensure that research participants do not only benefit from the result but also from the actual conduct of the research process. A good research study pays careful attention to the ways in which researchers interact with participants in the research. It is critical to consider the potential hierarchies and associated power dynamics that may arise.

During the interview

- The collection of data from participants requires the employment of sensitive and appropriate methods. The researcher shall be in close collaboration with the participants and is enjoined not to have only an instrumental but a genuine relationship with the participants. This rejects the concept of “detachment” of the researcher from the research participants’ problems. Treating research participants as human beings will entail a degree of emotional involvement and create a bond between the interviewer and respondent that can potentially empower both, without creating or fostering dependence.
- This entails that the researcher listens to the research participant with sensitivity. Participants who have experienced violation and trauma may react poorly to questions around their experiences; the researcher should be able to recognise this and provide an appropriate response.
- The interview should be conducted by a woman member of the research team.
- During the course of the interview, the interviewer should introduce any section enquiring about violence carefully, forewarning the respondent about the nature of the questions and giving her the opportunity to either stop the interview, or not to answer these questions.
- Collaboration with the participants means also that the researcher is willing to self-disclose – to share her/his experience if the participant so requests.
- The researcher must refrain at all times from any conduct or statement that has the effect or impact of blaming the woman for the violence she has experienced.

Boundaries

- Researchers shall take steps to address other needs of the participants such as counselling and psycho-social and emotional support through referrals to local and culturally appropriate resources. However, researchers shall be explicit regarding their limitations, and not make grand promises or offer false hopes to participants.
- Interviewers should not take on a role as counsellor, and any counselling activity that may be offered in the context of the study should be entirely separate from the data collection.
- Interviewers should be open to assisting the respondent if asked within the limits of these protocols, but should not tell her what to do or take on the personal burden of trying to “save her”.
- Variations in individual and cultural understandings of what constitutes violence against women (including rape, marital rape, assault, harassment, etc.) are to be expected. The researchers’ role in working with victims/survivors of violence (as well as all other interviewees) is to bring out their own understandings of the violence they experienced (or witnessed or participated in), through questions and sharing of perspectives that provide room for conversation around different views – rather than trying to stick with a pre-determined definition/understanding of what constitutes violence, rape, harassment, assault, etc.
- Researchers should distinguish themselves as “researchers” in this project, and their role as “advocates” in their regular work. For the purposes of the research, it is not the researchers’ role to seek to uncover the “objective truth” of the cases being discussed; if conflicting accounts are provided by any of the respondents, these are documented, and inconsistencies can then be explored through the write-up and analysis of the cases.

Methods of contact between respondent and researcher

- Respondents should be able to contact the lead field researcher (i.e. the interviewer) to ensure consent throughout the research process. This could be the telephone number of the partner organisation or a cell number unique to the research project, whatever poses less risk to researchers and survivors.
- Respondents should understand that the field research team can only provide support in the form of suggested resources (see below).
- Where few resources exist, it may be necessary to have a trained counsellor or women's advocate accompany the interview teams or provide support on an "as needed" basis. Generally this can take the form of alerting participants that a staff person trained in counselling for women's and/or violence issues will be available to meet with anyone who needs it or is interested at a set time and place. (Preferably this location should be a health centre or local organisation where women can easily go without arousing suspicion).

Providing referrals to social support services

- Prior to conducting the research, researchers need to meet with potential providers of support, which may include existing health, legal and social services and educational resources in the community, and less formal providers of support (including community representatives, religious leaders, traditional healers and women's organisations). This background research needs to be included in the timeline and budget before conducting any interviews.
- A list of such resources should be made available to each respondent, but only provided when asked for. Such a list should be framed as resources for "women's health" broadly, to minimise risks to participants that may result from possessing such a list.

C. Well-being and safety of the research team

1. Research on VAW can be emotionally exhausting, draining and almost overwhelmingly stressful. Research teams should be experienced in working with emotionally difficult material.
2. Support should be available to the research teams, such as regular debriefing and counselling when necessary. This could be encompassed by hiring an external counsellor to provide support on an "as needed" basis, both for participants (as mentioned above) and for the research team.
3. Predetermining safe spaces as possible locations for the interview can help provide security for the research team as well as respondents.
4. In some instances, the research may have to be conducted in the locale of the participant (for example in a remote or rural area) - and this may present unique security concerns. In such cases, researchers should try to schedule the interview at a time which provides ample room to travel at times that pose less risk to themselves (i.e. ensuring they can travel to and from the interview during daylight hours).
5. In all cases, a female member of the team should interview the victim/survivor directly. However, teams may need to include a number of male members to negotiate contexts where threats to

women's security appear to be acute. This has to be included in any budget and pre-assessment for participant selection.

6. For the purposes of this particular research project, we have neither the resources nor time to undertake research in extremely compromising situations – and cancelling on participants once we have engaged them in the process of joining the study presents ethical challenges. As such, all care must be taken to assess as fully as possible the potential security risks to both the research team and participant before confirming the selection of a case and scheduling an interview.
7. Researchers need a clear understanding of the actions they may be liable for in conducting this research, according to the laws in their own contexts – for example, whether the act of documenting and storing pictures or videos in the cases may make them subject to lawsuits under laws on “child pornography” or “voyeurism”, etc.
8. Researchers should outline for each case what the benefits, if any, would be of obtaining and/or viewing photos/videos that constitute the violent act, in addition to the risks. Researchers should decide whether it is crucial to their advocacy to obtain pictures/videos, or to view/watch them, and if so researchers must strive to keep advocacy efforts separate from the research project.
9. All research teams need to write up a risk assessment for each case, before pursuing it in the research project.

D. Protocols on data Collection, storage and transmission

Ensuring confidentiality

- Everyone involved in the research has the duty to assure the participants that their stories shall be kept confidential and their identities protected.
- Confidentiality in the research means that only the field research team has access to the participants' identity, but in all data collection and presentation methods, the participants cannot be identified by others. (By contrast, anonymity would mean that even field researchers do not know participants' names or contact information. Anonymity is usually guaranteed by different methods, such as population surveys).
- All participants will be asked to choose a pseudonym that will be used in research documentation, transcription, and dissemination. All narratives in this instance will have identifiable names (of places, people involved, etc.) changed so that neither the individual nor the community can readily be identified.
- We acknowledge that in some instances information about cases may be readily available in the public domain, and already considered “public” knowledge. In these instances, names will still be changed in the final write-up of the case studies, but we acknowledge that these cases will likely be identifiable to people beyond the research team.
- Video or photo documentation of participants will not be used for any reason during the research process.
- Participants shall determine what kind of information and details to share, no matter how crucial the women's revelation may be to the research.

Location of interview

- Interviews with women for case studies demand time and energy on the participants' part, and therefore should be carried out in settings that are most convenient for them and require the minimum amount of their time.
- Logistics planning should include consideration of respondent safety. This will require that the study's budget anticipate the likely need to reschedule some interviews. It should also include advance identification of additional locations (such as a local health centre) where interviews can be conducted if women so desire.
- Interviews should be conducted in complete privacy. In cases where privacy cannot be ensured, interviews should be rescheduled or relocated.

Collecting field notes

- No names should be written on field notes/log books/questionnaires. Instead, unique codes should be used to distinguish questionnaires. These do not need to be complicated, but ensure that those outside the research team will not be able to identify the respondent directly. This could be the pseudonym the interviewee chooses. Where the interviewee has not yet chosen a pseudonym, this could then be an interim code (for example, first three letters of the respondent's last name + first three letters of their city/village/district).
- Where identifiers are needed to link a questionnaire with the household location or respondent, they should be kept separately from the questionnaires, and upon completion of the research, destroyed.
- In all further analysis, the codes should be used to distinguish questionnaires. Participants should be informed of confidentiality procedures as part of the consent process.

Recording the interview

- Audio recordings should be made for the in-depth interviews with survivors of violence.
- The permission of the respondents should be sought before taping. The name of the respondent should *not* be included in the audio recording at any stage.
- Respondents should be informed of who will have access to the tapes and for how long they will be kept.
 1. In this case, only the interviewer (and transcriber, if different from the interviewer) will have access to the audio recording.
 2. The audio recordings should be kept in an encrypted file³² on an external hard drive, in a locked cabinet of the partner organisation, with limited access.
 3. The audio recording will be destroyed at the end of the FLOW/EndVAW project (January 2015).
 4. In addition to the interviewer, only the translator (if the interview is not conducted in English) and APC research team will have access to the transcript.
 5. If translators external to the APC research team are hired for the project, the protocols of their contracts will ensure that they destroy the transcript once translation is completed.
- Extreme caution must be taken to securely transport raw data from locations of interviews to places where data is processed. This applies to all recording media.

³² Use encryption software (e.g. TrueCrypt) to ensure security of the file.

- Encryption software must be used during all data storage to ensure security of the data. All contact details, recordings and transcripts of interviews, lists of interviewees, fieldnotes, etc. must be stored in an encrypted volume, both on personal computers, as well as on portable devices that are being used to transport data between computers.³³
- Sharing of such data is permitted only:
 1. Using a virtual private network³⁴ to share data that must first be encrypted by a stand-alone encryption software, OR
 2. Via email as OpenPGP-encrypted attachments. It is highly recommended that before such data is shared via email it is also encrypted by a stand-alone encryption application.

Transcribing the interviews

- The importance of recording and transcribing the interviews is to ensure that women's experiences and perspectives are shared in their own words. Relying on the interviewers' notes/memories may be insufficient to ensure the quality of data and its analysis.
- Transcribing the interviews also enables the respondents the option of reviewing the information they have provided if they wish, and choosing which information they consent to share with the final research and which information they wish to have omitted.
- Ideally, the interviewer is also the person responsible for transcribing the audio recording, to minimise transfer of the data.
- Particular care should be taken during the presentation of the research findings that the information presented is sufficiently aggregated to ensure that no one community or individual can be identified. Where case study findings are presented, sufficient detail should be changed to ensure that it is not possible to identify the source of this information.

8. Key terms, concepts and definitions

Violence against women (VAW)

The United Nations Declaration on the Elimination of Violence against Women (DEVAW) defines VAW as *"any act of gender-based violence that results in, or is likely to result in, physical, sexual or psychological harm or suffering to women, including threats of such acts, coercion or arbitrary deprivation of liberty, whether occurring in public or private life."*

We take this definition to include all those who self-identify as women, including transgender, transsexual and intersex women.

The root cause of VAW lies in unequal power relations between men and women in almost all facets of life.

Yet we recognise that gender-based violence affects people of all genders, as it is based on patriarchal moralising notions of "appropriate" gender roles, often limited to a heteronormative binary world view of girl/boy or woman/man.

Note: Though it is the most pervasive form of violence globally, VAW was only officially recognised as a violation of fundamental human rights in 1993 with the passing of the UN DEVAW. Women's rights

³³ TrueCrypt is a recommended free/libre open source application that can be used for encrypting data on your computers and portable devices.

³⁴ APC OwnCloud is the recommended network we will use (owncloud.apc.co).

activists have marked 25 November as a day against violence against women since 1981; the date was chosen in remembrance of the 1960 assassination of the Mirabal sisters, three political activists who opposed the Trujillo dictatorship in the Dominican Republic. The international community only officially designated 25 November as the international day against violence against women in 1999, with UN General Assembly resolution 54/134.³⁵

Technology-related violence against women

Following the UN DEVAW definition, this means any acts of gender-based violence intended to cause harm to a woman or girl that are mediated or perpetuated through the use of information and communication technologies (ICTs).

Technology-related violence against women happens in two ways:

- Technology is a tool used by the perpetrators to carry out acts of violence against women, either online or offline, or both (taking/uploading a video, “photoshopping” or altering a photo, blackmail). The victim/survivor does not necessarily know of/come into contact with the technology herself.
- A woman’s use of technology is targeted by others as a way to harass/intimidate/cause harm (e.g. harassment directed at her Facebook/Twitter/email account; she receives threatening text messages or WhatsApp messages; her private data is collected by hacking into her computer; monitoring and tracking her whereabouts; etc.).

Online safety and privacy

Online safety and privacy is about the right to communicate free of surveillance and interception (including the right to use encryption), and protecting one’s identity from being revealed to (or stolen by) third parties. In practice this means having the right to choose which information you reveal about yourself and the right to be online safely.

Online service providers (like social media sites) must ensure that their security and privacy policies are consistent with human rights standards, and that their users have the right to control their own data. Security and privacy are not an end-point, but a habit.

Online harassment

Harassment consists of the intentional crossing of your emotional or physical safety boundaries. You must have boundaries set in place clearly in order for that to apply. The legal definition of harassment, according to Black’s Law Dictionary, is:

"A course of conduct directed at a specific person that causes substantial emotional distress in such person and serves no legitimate purpose" or "Words, gestures, and actions which tend to annoy, alarm and abuse (verbally) another person."

This is of course a very broad definition, which state and federal legislation and common law have narrowed and refined in various ways. Online harassment consists of any actions that meet the qualifications of the above definition after the harasser has been told to cease using ICTs as the tool to

³⁵www.un.org/en/ga/search/view_doc.asp?symbol=A/RES/54/134&referer=/english/&Lang=E

perpetrate those actions (for instance, sending repeated SMS, sending threatening emails, etc.). Online harassment may or may not be of a sexual nature, and thus is broader than sexual harassment.

Sexual harassment

Unwelcome sexual advances, requests for sexual favours, and other verbal or physical conduct of a sexual nature. This could include activities such as posting pictures of a victim on websites, repeated emails of a sexual nature sent to the victim, or abuse of a position of power in the workplace.

Unwelcome behaviour is the critical phrase. Unwelcome does not mean “involuntary”. A victim may consent or agree to certain conduct and actively participate in it even though it is offensive and objectionable. Therefore, sexual conduct is unwelcome whenever the person subjected to it considers it unwelcome. Whether the person in fact welcomed a request for a date, sex-oriented comment, or joke depends on all the circumstances.

Harm

The harm and other consequences that victims/survivors of technology-related violence against women suffer are very often diminished or disregarded in the heated public debates accompanying such incidents. Technology-related violence usually takes place online and unless it extends to the physical world, it mostly results in psychological and emotional harm, rather than physical violence. Harm can be either subjective (the fear of being harmed, for example) or objective (such as harassment or stalking). As yet, while some courts recognise objective harm, the subjective harm of, for example, privacy violations is largely unrecognised.

There are multiple types of harm experienced in instances of technology-related VAW, which include:

- Emotional harm
- Sexual harm
- Psychological harm
- Invasion of privacy
- Harm to reputation.

We recognise that the distinctions and understandings of “harm” and “violence” are not always clear, but for the purposes of this research we understand harm to constitute a part of violence. We recognise that violence occurs on a spectrum and ranges in severity by which it is experienced; e.g. from discomfort to harm to abuse to violence. Yet this spectrum is not necessarily linear, and the “severity” is often hard to objectively discern; for example, repeated and prolonged discomfort and harm is precisely a technique used to inflict abuse, violence and torture. This research will help explore the way harm is experienced subjectively by those whose rights have been violated, and how to create appropriate remedies around this.

Internet intermediaries

Internet intermediaries are the entities that 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.

Intermediaries may play more than one role, that is they may be intermediaries in one context, but not another. An example is a social networking platform, which is both the end product, but facilitates communication between individuals and groups. Intermediaries are distinct from “content producers”, which are the individuals or organisations who are responsible for producing information and posting it online

For the purpose of this research, we are limiting our focus to the following internet intermediaries: internet service providers (ISPs), web hosting services, social networking sites, and telecommunications companies (particularly mobile network operators). These intermediaries have been identified as most commonly implicated in the instances of technology-related VAW mapped by APC partners.

Internet intermediary liability

Liability for internet intermediaries refers to the legal obligations of internet intermediaries for the hosting and distribution of content produced by third parties. Most liability issues pertain to transmitting copyrighted material or classified information on matters of national security, or directly and knowingly participating in criminal or illegal activities.

However, internet rights advocates continue to demand that internet intermediaries be shielded from liability for any content produced by a third party. At the international level, there is an increasing move towards “ethical responsibility” of internet intermediaries (and corporations in general), to act to uphold universal human rights and ensure that their companies’ actions do not infringe on or violate the rights of their users, and that they take all measures to ensure that their users do not infringe on or violate the rights of other users.

For the purpose of this research, we are not mapping the laws governing internet intermediary liability. We are following the Ruggie framework³⁶ for corporate responsibility to uphold human rights in policy and practice, and exploring how corporate policies and practices diverge from international rights frameworks. Importantly, this research may demonstrate how to take a more nuanced approach to internet intermediary liability; like all private actors, corporations cannot dictate the rules they play by alone and must be accountable to universal human rights principles.

Internet rights

The internet rights movement seeks to apply the framework of fundamental human rights in the current context of information societies. In a world where all aspects of life including economic, cultural, social and political life are increasingly mediated by technology, access to information technology for communication is critical to enable the realisation of a broad range of fundamental human rights. The right to communicate encompasses many other areas, such as freedom of opinion and expression, freedom of peaceful assembly and association, privacy, the right to development and women's rights.

Too often “internet rights” are pitted against “women’s rights”, in the way that once “human rights” were seen as completely separate from “women’s rights”, until finally after the 1993 Vienna Conference violence against women was brought to the international stage like never before. When discussing technology-related VAW we could easily compartmentalise the issue into one of “women’s rights”. Our research should contribute to de-compartmentalising these concepts, and building universal “users’ rights” that uphold principles of gender equality and denounce gender-based violence in its entirety.

³⁶www.ohchr.org/en/NewsEvents/Pages/DisplayNews.aspx?NewsID=11164

Due diligence

Due diligence refers to the level of care or activity that a duty-bearer is expected to exercise in the fulfilment of their duties. For various areas of law, standards of due diligence have been developed to provide a “measuring stick” with which to assess if a state or other actor is meeting the obligations that they have assumed. Using a rights-based approach, a due diligence standard serves as a tool for rights-holders to hold duty-bearers (such as states) accountable by providing an assessment framework for measuring whether the states have fulfilled their obligations. This is especially important where the potential infringement comes through a duty-bearer’s failure to act, as it can be difficult for rights-holders to assess if an omission constituted a violation of their right without some normative basis for the appraisal.

The due diligence standard for violence against women (VAW) is laid out in the Declaration on the Elimination of Violence against Women (1993) in Article 4(c), where states are urged to “exercise due diligence to prevent, investigate and, in accordance with national legislation, punish acts of violence against women, whether those acts are perpetrated by the State or by private persons.” The Committee on the Elimination of All Forms of Discrimination against Women (CEDAW) noted in its General Comment No. 19 that “States may also be responsible for private acts if they fail to act with due diligence to prevent violations of rights or to investigate and punish acts of violence.”

Access to justice

At the international level, access to justice is a fundamental right guaranteed under Article 8 of the Universal Declaration of Human Rights: “Everyone has the right to an effective remedy by competent national tribunals for acts violating the fundamental rights granted him by the constitution or by law.” The right to access to justice is also guaranteed by other international human rights instruments such as the International Covenant on Civil and Political Rights (ICCPR) and the International Covenant on Economic, Social and Cultural Rights (ICESCR). Particularly for women, the Convention on the Elimination of All Forms of Discrimination against Women (CEDAW), together with its Optional Protocol and General Recommendations 19 and 25, assures the right to access justice.

For the purposes of this research, we are following the Access to Justice Framework elaborated by the Women’s Legal Bureau-Philippines. This framework sees the need “to look beyond legal measures and into the interplay of politics, economics, and culture in women’s access to justice in cases of violence. Looking alone at the existence of laws protecting women, the availability of legal aid and counsel and at the process of adjudication and enforcement as a frame for access to justice for women victims of violence would be limiting. It would fail to address the subordinated and subjugated identities of women in law and in society. It would fail to account the structural inequalities between men and women, the systemic and historic disadvantaged position of women, the culture of impunity in cases of VAW, and the prevailing gender bias and system of patriarchy that continue to persist in the judicial system and in society.”

A fuller discussion of the Access to Justice Framework can be found in the research methodology section of the research design. The original framework is available at:

www.ohchr.org/Documents/HRBodies/CEDAW/AccessToJustice/WomensLegalAndHumanRightsBureau.pdf

Anti-VAW legislation

A law or group of laws that criminalise acts of violence that disproportionately affect women. While many countries have various pieces of legislation that deal with different types of VAW (such as rape, domestic violence, etc.), the Philippines by example has one law that deals with all types of violence against women, labelling it as such. This has the advantage of making clear the gender-based nature of such violence, locating it in the power differential between men and women, and thus helping to uncover the root causes of the violence. Another value of anti-VAW laws as far as technology-related VAW is concerned lies in the inclusion of alternative forms of violence such as psychological violence which include intimidation, blackmail, verbal attack, insult, profanity, humiliation and threat.

Remedy

Remedy is the means by which the violation of a right is prevented, redressed or compensated. Generally, the right to a remedy should include: access to justice; reparation for harm suffered; restitution; compensation; satisfaction; rehabilitation; and guarantees of non-repetition and prevention. Remedy can operate at different levels. For the purpose of the FLOW/End VAW project we focus on two types of remedies – legal remedies operated by the state, and remedies operated by internet intermediaries (such as through their terms of service, which may or may not extend into the legal realm).

In assessing women's and girls' access to justice, this research will also uncover personal remedies operated by those who have had their rights violated and civic remedies operated by individuals, communities, or civil society actors engaging on the survivor's behalf.

Domestic legal remedy

This shall refer to the existence of laws addressing a particular harm/violation, the enforcement of said laws through investigation and prosecution, and the trial of the same through judicial processes. It shall likewise cover relief provided by the state; state laws, policy frameworks and justice mechanisms maintained or operated by the state and its agents; and other mechanisms where state authority is directly involved either in creation or administration.

Corporate response mechanisms

This shall refer to remedies provided by internet intermediaries e.g. internet service providers, search engines and portals, data processing and web hosting providers and participative networked platforms such as complaint mechanisms, corporate user policies, etc. This could be as simple as having a "report" or "block" option for users, or as extensive as collaboration with law enforcement agencies in providing information for prosecuting cases or obtaining restraining or protective orders, etc.

Corporate policies

Corporate or company policies are written statements corporations make that guide their work, including on matters such as right to privacy (for both employees and customers), terms of service and right to redress through the courts.

The Special Representative of the UN Secretary-General on the Issue of Human Rights and Transnational Corporations and Other Business Enterprises has recommended a framework for corporate responsibility and accountability based on three principles: "protect, respect, remedy". Popularly known as the Ruggie

framework (after the Special Representative John Ruggie), the framework was announced in 2011, and has been endorsed by several key bodies and institutions.

Reporting a case vs. filing a case

Depending on the law of a particular country, reporting a case could mean reporting the incident to the relevant authorities to keep a record such a police blotter and no further action was taken, while filing a formal complaint involves a cause of action that sets out the facts and legal reasons for one person to file a case against another person or party and as such includes a demand for investigation, prosecution and relief.

Protection order

Depending on the law of a particular country, it is an order issued in cases of VAW to safeguard/protect the woman from further harm.

Restraining order

Depending on the law of a particular country, it is a general form of protection order or legal injunction that requires a certain person/party to refrain from certain acts.

Legal processes

These refer to both events and actions that follow some prescribed procedure, namely filing a formal complaint to the police or court, investigation and prosecution.

III. Research instruments

1. Check list for mapping domestic legislation

Note: This instrument is to be used to affirm, substantiate and add to the preliminary domestic legislation mapping already carried out by the Women's Legal Bureau (WLB) for each partner country. WLB's mapping of each country context will be shared with each partner individually.

Partners are not expected to write another report based on this check list; rather partners can use the questions in this check list to review the mapping done by WLB, and to add details and commentary on laws and provisions that are either incomplete or missing from the original mapping.

The check list looks at substantive national-level laws, specifically laws to counteract violence against women (VAW), as well as ICT-related laws. The mapping also seeks to identify the specific provisions that can be invoked and used in cases of technology-related VAW. The domestic legal remedies mapping also provides room to discuss the political-legal context of the country in a short summary of the legislative system, how laws are passed, whether certain regions have autonomy and resulting challenges in terms of jurisdiction, etc.

1.1. Check list

1. Does your constitution guarantee human rights and fundamental freedoms?
 YES NO
2. If yes, enumerate the specific articles and their wording.
3. Are there law/s that guarantee women's equality and rights?
 YES NO
4. Enumerate the law/s that explicitly recognise equality of women and their rights.
5. Is violence against women (VAW) recognised in your country?
 YES NO
6. Enumerate the law/s that recognise VAW and provide definition thereof.
7. What are the specific provisions in these VAW laws that can be used and invoked in cases of technology-related VAW?
8. Do you have specific law/s that recognise technology-related VAW?
 YES NO
9. What is the law/s that recognise/s technology-related VAW?
10. Enumerate the acts of technology-related VAW identified as offences in the law/s.
11. What ICT laws (e.g. cybercrime, privacy, e-commerce, etc.) do you have?
12. What are the specific provisions in these ICT laws that address technology-related VAW?
13. What are the specific provisions in these ICT laws that address internet intermediary liability (particularly in regards to what content they are liable for)?

14. Aside from VAW laws, technology-related VAW laws and ICT laws, what do you think are the other laws that can be used in cases of technology-related VAW (e.g. anti-hate speech, anti-discrimination law, etc.)?
15. Identify the specific provisions in these other laws that can be used and invoked in cases of technology-related VAW.
16. Are there pending or emerging laws in your country that deal with VAW, ICT or technology-related VAW?
____YES ____NO
17. Do you know of any pending and emerging laws in your country that deal with VAW, ICT or technology-related VAW?
____YES ____NO
18. What are the pending and emerging laws? Please provide a brief description of the laws.
19. What international agreements/laws is your country signatory to that can be invoked in cases of technology-related VAW? (e.g. UDHR, CEDAW, DEVAW, ICCPR, CAT). Name of the law, the date signed by your country, the date ratified, and any reservations your country made upon signing.

1.2. Contextual background and critical analysis of national legislation

Note: These further questions should help guide partners in adding background context to the domestic legal remedies mapping already conducted by the Women’s Legal Bureau-Philippines, as well as providing a space to discuss the strengths and weaknesses of these laws.

I. National-level contextual background

- Brief summary of the legislative system in place:
 1. How are national laws passed? What are the governing bodies (parliament, upper and lower houses, etc.)?
 2. Is the system perceived as transparent and effective, particularly by women’s rights activists?
 3. Is it a federal system? Do provinces/states/municipalities have autonomy from national legislation?
 4. How are municipal/provincial/etc. laws passed? What are their governing bodies? Are municipalities/provinces/etc. still bound by the national constitution/charter of freedoms/national-level laws, and can they be held accountable at the national level for laws that directly go against the rights guaranteed at the national level?

II. National legislation that can be used to facilitate women’s access to justice in cases of technology-related VAW

i. Specifically in relation to women’s rights, civil rights and VAW

Note: When adding to the mapping by WLB, please include direct excerpts and exact wording of the laws wherever referencing pertinent articles/sections. Please include this in your local language, and where available in English provide the official translation beneath. If an official translation is not available, please provide a rough translation underneath the original excerpt, and note it as such.

Example:

- Constitution (date passed)
 1. Specific articles pertinent to women’s human rights and technology-related VAW (privacy, hate-speech, etc.)
 2. Any commentary on its strengths and weaknesses in guaranteeing women’s rights (e.g., privileges only certain religious or ethnic groups, doesn’t explicitly guarantee women as full and equal beings, doesn’t guarantee basic access to healthcare and education, etc.)
- Family laws (date passed)
 1. Specific articles pertinent to technology-related VAW
 2. Any comments on strengths and weaknesses in guaranteeing women’s access to justice (e.g. paternalistic view of women’s rights as subservient to their male family members, should be changed to reflect “x”, etc.)
- Anti-VAW law (date passed)
 1. Specific articles pertinent to technology-related VAW, the punishments for those who perpetrate VAW (maximum and minimum sentences, years in prison, etc.)

2. Any commentary on its strengths and weaknesses in guaranteeing women's access to justice (e.g., looks at women as victims, doesn't recognise rape or domestic violence, etc.)
3. Any commentary on the punitive measures and how they might be improved/changed (based on debates and discourses amongst women's rights and civil society groups, etc.)

Etc., based on the results of the mapping.

ii. Specifically in relation to ICTs and VAW

Note: Where it is apparent, include articles that hold internet intermediaries liable for certain content.

- Anti-child pornography act (date passed)
 1. Specific articles pertinent to technology-related VAW (including intermediary liability, individual liability, sharing of data, privacy, etc.)
 2. What are the relevant punitive measures for committing the criminal actions under the law (maximum and minimum sentences)?
 3. Commentary on the perceived problems with the law (e.g., too easily leads to the criminalisation of and censorship of sexuality, particularly youth's sexuality)
 4. Any comments on strengths and weaknesses in guaranteeing women's access to justice (e.g. only applicable in certain municipalities, but not national level).

Etc., based on the results of the mapping and whatever pertinent laws are identified.

2. Check list for mapping corporate user policies

This is a guide to mapping the corporate user policies of internet intermediaries (social networking sites, mobile phone network operators, web-hosting services) by identifying the specific provisions in policies that can be invoked and used in cases of technology-related VAW. Much of this information should be found through desk-research and on the websites of the corporations. Some details might have to be uncovered through telephone interviews with a corporate representative from the policy department. The "policies" outlined below are general categories, and the specific names of the policies for each intermediary may be different. Please document the exact name of the policies you refer to in your mapping.

1. Name of the internet intermediary you are mapping and link to its website: _____.
2. Outline in brief the general services it provides, the location of its headquarters, and where it operates (including if it is local, regional, national or transnational): _____
3. Briefly outline what policies and provisions the intermediary has in place with regard to the following (note: wherever possible provide the link to the policies online, and include the precise wording of the most pertinent provisions here where applicable):

A) Terms of Use (may also be "Acceptable Use", "Community Standards", "Statement of User Rights and Responsibilities", etc.)

Does the policy explicitly prohibit:

- Hate speech? How is hate speech defined?
- Rude or offensive comments?

- Personal attacks on others?
- Invasion of another person's privacy (i.e. collecting or storing personal data about other users, or stalking or harassing another person or entity)?
- Graphic violence?
- Pornography?
- Abuse? How is abuse defined?
- Is there specific reference to prohibiting abuse or harassment or hate speech, etc. on the basis of sex, gender, race, ethnicity, ability, religion, etc.?

B) Content regulation (may overlap with Terms of Use/Community Standards)

- What content is permitted?
- What is prohibited?
- Is there a specific distinction between what content is prohibited (may violate terms of use or community standards) and content that is considered illegal or criminal, and thereby punishable by law? What laws are mentioned?
- Is there any reference to the internet intermediary's liability for particular content? If yes, under what laws?
- What are the mechanisms in place to block, filter or remove prohibited content?
- How many people need to report or "flag" content as inappropriate before the intermediary reviews the content?
- What are the steps taken in regards to the user who has generated the prohibited content?
- In cases where content is removed but it does not actually violate the terms of use, what mechanisms are in place to have the decision reversed and the content re-instated?
- What department or committee decides what content is taken down?
- What mechanisms are in place to carry out such a decision?

C) Privacy and Confidentiality

- How is user data used, received, generated, stored, collected and shared?
- What personal details of the user does the intermediary store?
- What control do users have over their own data? (i.e. what can they choose to keep private, and what do they have no control over?)
- Under what conditions is data handed over to third parties, including law enforcement? (Note: Here we would ideally like to see an explicit statement of the conditions in which data can be handed over to law enforcement, rather than just a general statement of "we hand over data in accordance with the law".)

D) Safety/Reporting/Violation of Terms of Use

- Does the intermediary outline “safety guidelines” for users?
- What is the reporting procedure for someone who feels their rights have been violated? (e.g, completing a form online, contacting a specific department [complaints, safety, etc.] via telephone or online or in person)
- What is the reporting procedure to ask for content to be blocked or taken down?
- What is the procedure for law enforcement to obtain information in the case of illegal activities?
- What remedies does the intermediary state it may take in cases of violation of the terms of use?
- What laws does the intermediary express it is governed by? (Which country? Which specific laws?)
- What is the intermediary’s position on cooperating with law enforcement outside its national jurisdiction?

3. Informed consent form for victims/survivors

Note: In cases where victims/survivors may be unwilling to sign a consent form, researchers must ensure that all of the information in the consent form is explained in simple and understandable language to victims/survivors, and have some way of documenting that (verbal) consent to participate was obtained. Researchers also need to outline the means by which victims/survivors may contact you during the research, especially to provide the opportunity to withdraw their consent before finalisation of the research.

Importantly: this consent form is specifically for victims/survivors interviewed, to whom we have greater responsibilities in the research than other respondents, given the nature of the information victims/survivors are sharing with us and the risks they face of re-victimisation, or increased or new threats to their safety for participating in the research.

However, informed consent must be obtained from all participants who give interviews specifically about the case. They must understand that the information they provide may be published, but that their individual names will be changed and identities kept confidential. Where the case is already in the public discourse, researchers must explain that despite the changing of names, there is a risk that others may be able to identify the individuals involved, and that only if they understand this risk should they consent to participate. All participants should understand that their interviews will be recorded, and this data will be kept secure by the research team (according to the Ethical Guidelines and Protocols), and destroyed upon completion of the project in January 2015.

Consent to participate in “Ending Technology-related Violence Against Women”

(A) Purpose of the interview

This interview is being carried out as part of a research project on “Ending Technology-Related Violence Against Women”. The research team will interview about 20 women who have experienced rights violations or abuse mediated through technology.

The aim of the interview is to document women’s experiences of technology-related violence, and explore whether women have been able to stop the violence and access justice. We will use the research to advocate for new policy and laws that improve women’s access to justice when technology related violence against women occurs.

This research is a collaborative effort between the Association of Progressive Communications international network, and __(name of national partner organisation here)__.

(B) Procedures of the interview

The interview should last about one hour, and is a combination of yes/no answers and open-ended questions.

The interview will be audio-recorded and transcribed. Only the research team will have access to the recording and transcript. The information will be stored on a secure hard drive, and kept until the completion of this project in January 2015. After this, the recording and transcript will be destroyed.

Your identity will remain confidential. This means that the researchers will know your name and contact details, but this will not be shared with anybody else. All names – including of your village/town, of people involved in the case – will be changed when the information is shared in our reports.

You may ask for a copy of the transcript. You may ask for any of the information to be excluded. You may withdraw from the study at any point prior to our publishing the final report in April 2014.

You may ask questions of the interviewer at any time during the interview. You may also choose to stop the interview at any time if you experience discomfort while completing the interview.

(C) Risks and benefits

- Some of the questions asked during the interview will require that you reflect on times where you (or people close to you) experienced discrimination or abuse, and this may cause emotional distress.
- The researchers have a list of resources, including the numbers of help phone-lines that you can obtain upon request.
- To minimise the risk of social stigma for participating in the study, your participation will remain confidential.
- If you change your mind about any of the information you have shared, you can ask that it be omitted (removed) from the transcript and for that information to be destroyed.
- Participating in this interview hopefully gives you the opportunity to discuss relevant issues that affect your life, to voice concerns and to share your stories in a context that encourages that.

(D) Conditions of participation

- I understand that I am free to withdraw my consent and discontinue my participation at any time without negative consequences.

- Should I withdraw from the study before April 2014, all data (audio, digital and written) related to my participation will be destroyed. All other data will be confidentially housed in *_(partner organisation's)_* possession until January 2015, after which all data will be destroyed.
- I understand that my participation in this study is **confidential** (i.e., the researcher will know, but will not disclose my identity).
- I understand that all names of people and places mentioned during the interview will be changed to ensure confidentiality.
- I understand that the data resulting from this study will be published, and that the work might be presented at future conferences for the purpose of advocacy against technology related VAW.

“I have read the above statement and have been fully advised of the procedures to be used in this project. I have been given sufficient opportunity to ask any questions I had concerning the procedures and possible risks involved. I understand the possible risks involved and I assume them voluntarily. I likewise understand that I can withdraw from the study at any time.”

Respondent signature

Date

4. Semi-structured interviews of victims/survivors

Note: This research instrument can be delivered in two ways as a guide in: a) direct interview with victim/survivors and b) review of secondary sources such as news reports, online articles, etc. Include in the wrap-up of the interview the opportunity for participants to express and discuss how they feel about having given the interview and contributing their stories to the research.

4.1. Background to the Interview

This interview will take at least one hour. This is a check list-type interview wherein there is an assumption that the researcher made a background study about the case prior to the interview and would just have to further probe on the answer of the victim/survivor if it is not clear. However, the length of the interview would depend as well on the victim/survivor and how open and comfortable she is in answering the questions. It is important that the researcher establishes a rapport with the victim/survivor and puts her at ease while interviewing.

Informed consent: Before conducting the interview, an informed consent form should be signed, and all the details of the research explained to the victim/survivor, including that the interview will be recorded and transcribed, that the details may be published, and that she has the right to stop or withdraw from the interview/research without consequence.

Overall objective: The main objective of the research instrument is to surface women’s voices and experiences in seeking domestic legal remedy, as well as seeking redress directly from the internet intermediaries involved, in cases of technology-related VAW.

This is divided into three sections, namely a) the profile of the woman, b) the violation she experienced and c) the domestic legal remedy she accessed, each with its own specific objective.

Definition of terms

The researcher should keep in mind the operational definition of the following terms and should be guided accordingly when explaining the terms to the victim/survivor.

Domestic legal remedy: This shall refer to the existence of laws addressing a particular harm/violation, the enforcement of said laws through investigation and prosecution, and the trial of the same through judicial processes. It shall likewise covers relief provided by the state; state laws, policy frameworks and justice mechanisms maintained or operated by the state and its agents; and other mechanisms where state authority is directly involved either in creation or administration.

Corporate remedy: This shall refer to remedies provided by internet intermediaries, e.g. internet service providers, search engines and portals, data processing and web hosting providers and participative networked platforms such as complaint mechanisms, corporate user policies, etc.

Internet intermediaries: Internet intermediaries are the entities 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. Intermediaries are distinct from “content producers”, which are the individuals or organisations who are responsible for producing information and posting it online. For the purpose of this research, we are limiting our focus to the following internet intermediaries: internet service providers (ISPs), web hosting services, social networking sites, and telecommunications companies (particularly mobile network operators).

Reporting a case vs. filing a case: Depending on the law of a particular country, reporting could mean reporting the incident to relevant authorities to keep a record such a police blotter, and no further action was taken, while filing a formal complaint involves a cause of action that sets out the facts and legal reasons for one person to file a case against another person or party and as such includes a demand for investigation, prosecution and relief.

Protection order: Depending on the law of a particular country, it is an order issued in cases of VAW to safeguard/protect the woman from further harm

Restraining order: Depending on the law of a particular country, it is a general form of protection order or legal injunction that requires a certain person/party to refrain from certain acts

Legal processes: These refer to both events and actions that follow some prescribed procedure, namely filing a formal complaint to the police or court, investigation and prosecution.

4.2. Interview questions

Profile

Objective: This section aims to surface the immediate contextual realities (social, economic, political) of women and find out how these realities affect women’s vulnerability to technology-related VAW and their capacity to seek remedy and access to justice. Knowing the immediate context of the victim/survivor will help in probing further on certain questions on domestic legal remedy. Asking the following information could be a means for the researcher to establish rapport with the victim/survivor (get to know each

other). However, the researcher should exercise care and sensitivity in asking for the information, as the victim/survivor may not readily provide answers.

- Age
- Gender/sexual orientation
- Marital status
- Number of children
- Ethnicity
- Disability (if any)
- Education
- Source of income (researcher can further probe by asking the victim/survivor for an estimate of her weekly or monthly income or by asking the regularity of her income.)

Can you describe the violation that you have experienced?

Objective: This section aims to identify the kind of violation experienced by the woman, and the platform/ICT used to perpetrate the violation. The questions shall also surface the concept of harm based on the woman's experience.

- Can you tell me about your particular experience of violence on the [internet - Facebook, mobile phone, etc.]?
- Probe for the "facts of the case"
 - o How did it start?
 - o What platform or technology was used to commit the violation?
- Do you know the perpetrator/s?
 - ___ Yes
 - ___ No
- If yes, what kind of relationship do you have with the perpetrator/s?
 - ___ husband/live-in partner
 - ___ boyfriend/partner
 - ___ admirer/suitor
 - ___ friend
 - ___ family member or relative
 - ___ neighbour
 - ___ co-worker
 - ___ classmate/schoolmate
 - ___ Others (specify) _____
- How did the incident affect you emotionally, physically and mentally?
 - ___ Anxiety and fear
 - ___ Feeling a lack of safety

- Mental instability (loss of memory, difficulty concentrating, difficulty remembering exact details)
- Nightmares
- Sleep difficulties
- Feelings of intense distress
- Physical reactions (pounding heart, rapid breathing, nausea, muscle tension, sweating)
- Irritability
- Anger
- Guilt, shame, or self-blame
- Depression and hopelessness
- Embarrassment and feelings of exposure
- Feeling reputation was damaged
- Sense of privacy obstructed
- Feeling violated (physically, sexually, emotionally)
- What was the effect of the incident on your:
 - o Work - did it affect your work/ability to perform work? Please describe how [note that some may be housewives or do not have productive work. In such cases, ask whether the incident affected their ability to perform reproductive work (household chores, rearing children, foraging, etc.)]
 - o Studies (in case it happened to students)
 - o Relationship with family, friends and others - in what ways were they affected by the incident? Did you feel any of the following towards them?
 - Avoidance of people events or situation
 - Afraid of them
 - Lock myself in the house/confine to myself
 - Feeling freedom of movement was generally restricted
 - Feeling alienated or alone
 - Detached or estranged from them
 - Feelings of mistrust or betrayal
 - Feeling like I have to stay silent and not discuss the issue (feeling censored, or self-censoring)
- Have you had hesitations in using ICT because of what you have experienced? [Probe why she had hesitations, or how her use of ICT, or perspective on ICT, has changed because of the experience.]

Domestic legal remedy

Objective: This section is divided into two parts. The first part aims to render women and their experiences visible by looking at the factors that enable them to seek remedy such as women's awareness of the available options they have, their capacity/capability to make decisions and the

enabling conditions that allow them to seek redress. The second part aims to describe the actual experience and legal processes and procedures that women went through.

Part I: Available options

1. As far as you know, what are the options that you can take to address the abuse or violence that you experienced? Please provide as much detail as possible:

Laws (e.g. sexual harassment laws, violence against women laws, cybercrime laws, etc.).

Please name them, and the sections that apply if you are aware of it.

User policies and agreements and complaints mechanisms by internet service providers or telcos (e.g. report abuse button, etc.)

Others (deleting the account, ignoring the abuse, etc.)

2. Are you informed of the legal processes you may undertake?
3. How did you find out about the kinds of action you can take to address cases of abuse and violence related to ICT?

Researched on your own online or over the internet

In the media - news, television, radio

Overheard from someone

From government announcements

You know someone who experienced the same thing

Others (specify) _____

4. What actions did you take to deal with the abuse or violation?

Reported and/or filed a complaint to relevant authorities:

School/University

Office human resource department

Police

Other government agencies e.g. National Human Rights Institutions, Women/Gender Commissions

Cybercrime investigation units

Internet intermediaries (telcos, ISP, Facebook, Yahoo, Google, etc.) through online complaints or contact form for internet service providers or customer service departments of national/local internet providers

Others

Filed a legal action in court, e.g. filed a criminal case against the perpetrator

Others (please specify) _____

5. Besides reporting and/or filing complaints, what kind of help did you specifically seek from the relevant authorities (whether authorities is internet intermediaries, school personnel, police, legal workers, social workers, etc.)?
- Counselling
 - Technical advice
 - Legal rights (please explain)
 - Seek protection order and/or restraining order
 - Remove content and/or take down the content page photos or videos, comments page
 - Others (please specify) _____
6. What were the factors that you considered in making such actions?
- Cost e.g. affordability
 - Clarity of the law and legal processes
 - Technical knowledge
 - Confidence in authorities to understand my problem
 - Time e.g. personal time
 - Support from friends and/or family and other people
 - Awareness and knowledge of my rights
 - Others (please specify) _____
7. Did you make the decisions on your own or act on your own? For example, who made the decision to file the case? Or to report the case to internet intermediaries?
8. Did you consult someone regarding your decision? Who did you consult?
- Family and relatives
 - Friends
 - Law enforcement agencies
 - Lawyer
 - Colleagues
 - Others (please specify) _____
 - None
9. In reporting a case to internet intermediaries did you request assistance from a government agency to facilitate your complaint?
- Yes
 - No
10. In filing a case to internet intermediaries did you request assistance from a government agency to facilitate your complaint?
- Yes

No

11. What results did you get from your actions? How did the relevant authorities respond to your actions?

The police investigated my case immediately. On the same day that I filed a case, a person or team was assigned to look at my case and/or within a week the police started investigating my case.

A compensation was awarded to me.

I was given a protection order.

A new policy was issued because of my case.

They dismissed my complaint and advised me to not take any further action

They carried out investigations into the different agencies involved (e.g. police contacted relevant telco, cybercrime unit investigated website provider, etc).

Internet intermediary (telco, social networking provider, etc) blocked the abuser from further contacting me.

Abusive/offensive content (photo, video, comment, messages, etc.) was taken down or removed by the website and/or social networking site providers.

Access to accounts was reinstated.

New complaint mechanism was developed or improved because of my case.

I did not get any response from them.

Others (please specify) _____

12. How long after your initial report to the relevant authorities was the matter resolved (or if not resolved, when was a response was given)?

Please write down an estimation of how long it took (e.g. less than 1 week, within 6 months, more than 2 years, still in the process of resolution, etc.), in each instance. If multiple authorities were involved, recount the response process and response time with each authority – police, social service provider, internet intermediary, etc.)

13. If there was little follow-up from the relevant authorities, did you follow up with them to push the issue? Why/why not?

14. Did you look for help elsewhere or organise on your own to bring attention to your case? What was the response?

Part II: Awareness of rights and enabling environment: This section aims to find out how her awareness of her rights enables her to access domestic legal remedy.

1. Are you aware of your human/citizen's rights? of women's rights? of your rights as an ICT user? Can you give examples? [Probe the following: right to privacy, non-discrimination, right to information, freedom to express opinion, freedom of expression.]

- Would you say that you are able to exercise these rights through the use of [ICT] or not? In what ways? Can you give concrete examples of situations where you think you were able to exercise these rights?
- What hinders you from exercising these rights?
- What are the factors that enable you to exercise these rights?
2. What law or policy did you use to file a legal/formal complaint? Specifically cite the law/policy.
 3. Did the law or policy specifically identify the violation that you have experienced (technology-related VAW) and provide a procedure therefore?
 - Yes
 - No
 4. What was the specific provision (section/part/portion) of the law/policy that addressed your case?
 5. What were the factors that you took into consideration in filing a legal complaint?
 - Accessibility: police and court are geographically near my place
 - Cost: free legal aid and assistance was available to me
 - My safety: possible threat to my security and family
 - There were people and support groups who were ready to help/assist me
 - Others (please specify) _____
 6. What were the factors that you took into consideration in reporting to the internet intermediaries?
 7. Were your roles in the case and the process involved clearly explained by the relevant authorities (whether police and courts, or internet intermediaries, or both)? How clearly did you understand about your rights and the processes involved?
 - Clearly understood. I was always consulted and involved in the whole process.
 - I had an understanding of my situation. They consulted and involved me from time to time.
 - I did not understand anything. I let them make all the decisions for me.
 8. Did someone represent you in the case? Who made the decision as to who will represent you?
 9. Did you avail support services such as the following?
 - Counselling
 - Psychosocial therapy
 - Medical support
 - Shelter
 - Others (please specify) _____
 10. Who administered these support services?
 - Government
 - Non-governmental organisations (identify the particular nature and service provided by NGO)
 - Private institutions

Others (please specify) _____

11. How were the services able to help in your case as a victim/survivor of technology-related VAW?

Explained to you about the law and your rights

Explained to you about the technicalities of the case

Accompanied you to file a police report

Conducted their own investigation

Helped you get legal representation

Others (please specify) _____

12. What were the limitations that you have encountered in availing the support services?

Availability and accessibility: geographical distance of support services (far or near), applies only to certain groups or individuals

Cost: both direct costs of availing the services (transportation cost, cost of service itself, whether affordable for women or not) and indirect costs (absence from work, etc.)

Resources: lack of facility, lack of funds, lack of staff

Competency and gender sensitivity of the staff

Tedious or many requirements in order to avail the services

I went to many processes/procedures that I don't even understand.

Safety/security issues: the shelter did not provide enough security as the service providers; my safety was compromised in the shelter

Others (please specify) _____

13. What were the limitations that you have encountered in using the law or policy?

The law/policy did not explicitly mentioned technology-related VAW as a criminal offence

The law/policy did not provide protective mechanisms for victims

The law/policy did not provide clear procedures for investigation and prosecution of technology-related VAW

This was the first time the law was used for technology-related VAW

There is no jurisprudence yet as to the applicability of the law on technology-related VAW

Others (specify) _____

14. Were you satisfied by the response from the internet intermediary in your case? Why/Why not?

What would you have liked to see as the ideal outcome with the internet intermediary?

15. What are the difficulties you encountered while going through the legal processes, e.g. filing a complaint, investigation, prosecution, etc.?

Difficulty in identifying or absence of a specific remedy/law/legal process to address the harm

Availability and accessibility: geographical distance of state institutions and mechanisms, or linguistic barriers, e.g. language used in state institutions and in laws

- ___ Cost: both direct cost of availing state mechanisms (filing fees, attorney's fees, transportation, etc.) and indirect costs (absences from work, etc.)
- ___ Resources: lack of facility, lack of funds, lack of staff of state institutions and mechanisms
- ___ Lack of competency and gender insensitivity of policemen, investigators, prosecutors, judges
- ___ I went to many processes/procedures that I don't even understand.
- ___ Others (please specify) _____

16. Did the legal process help you? In what ways?

17. Are you satisfied with the results of your case? In what ways?

___ Do you feel you have attained/received justice? Why or why not?

___ What could have been an ideal or fair result for you?

18. Would you give the same penalty if the violation you experienced was done "offline", or should it be higher? Why or why not?

19. Do you have suggestions or recommendations to improve the process?

20. What lessons (or realisations) have you learned from your experience and would you like to share with other women and girls who may have a similar experience or case?

21. What recommendations can you give to the government or relevant authorities and service providers (internet intermediaries, schools, community groups, social workers, etc.) so that they can be of service or help to women, particularly to those who went through a similar experience as you?

5. Semi-structured interview for law enforcers involved in the case

Objective: The purpose of the interview is to know more about the police process, investigation procedures and how law enforcers respond to VAW and specifically technology-related VAW, paying attention to their attitudes towards victims/survivors. This should be able to surface how such processes, procedures and attitudes facilitate or impede women's access to justice.

Understanding the situation on violence against women (technology-related VAW)

1. What kind of investigations or cases do you handle? What kind of services do you or your agency provide?
2. How often do you receive reports and cases of violence against women?
3. What are the common cases you receive? Who are the perpetrators? Who are the victims? [Do they map victims' gender, ethnicity, class, etc. and do they get a sense of the trends in who is reporting?]
4. What is the trend in frequency and number of reported cases? Is it increasing or decreasing?
5. What are the major challenges in handling cases of VAW?
6. Do you receive or encounter cases of technology-related VAW?
7. If yes, what are the common cases reported to you?

8. How do you handle these cases? Are there existing laws specifically dealing with technology-related VAW? If yes, what are these laws? Are they considered criminal offences?
9. Are there existing policies or protocols that can be applied to investigate and prosecute technology-related VAW?
10. Is there a protocol as to who should handle, assist, interview victims/survivors? Who should do the investigation of the case? Is there a specific desk or unit within the agency that can handle technology-related VAW?
11. Is there a policy stating the criteria/qualifications for persons handling VAW cases, such as undergoing a series of training on gender sensitivity and VAW?
12. Is there a protocol on how to investigate/write reports on VAW? Do you have a separate logbook for VAW/technology-related VAW cases? Do you follow a particular format so as to have an easy reference and understanding of the case? Please describe the protocol.
13. Has there been any legal action taken in relation to technology-related VAW complaints? Can you describe these cases? What is their current status?
14. What are the services available for victims/survivors of technology-related VAW?
15. Do you have a referral system wherein victims/survivors of technology-related VAW are turned over to appropriate agencies? (Existence of agreement/coordination protocols with shelter, medical, psychosocial services, etc.)
16. If no, to your knowledge, has there ever been an incident of technology-related VAW such as accessing private data, taking photos/video without consent, stalking, changing/faking personal data, photos and videos, online harassment, threat of violence/blackmail, stealing identity, sharing and/or disseminating private information, abusive comments, trafficking, cyber sex dens, etc? What could be the possible options for the victims in these cases?
17. Do you think the current laws and policies are adequate to respond to possible cases of technology-related VAW? In what ways? In your opinion, is there a need for a new policy or law to deal with technology-related VAW?
18. What capacities (facility, personnel, office/agency) should the government have in order to deal with technology-related VAW? What can be improved?

6. Semi-structured interview with NGOs involved in the case

NGOs to be interviewed are those directly providing services to technology-related VAW victims/survivors and those who may not be providing direct services but whose works involve engagement in the field of women's human rights for a considerable length of time, particularly in addressing violence against women.

Objective: The objective of the interview is to gain insights on the issues of access to justice relating to technology related VAW.

1. Briefly describe the organisation, in particular its area of work and advocacies on women.
 - 1.1. What issues on women does your organisation engage in?

- 1.2. What kind of services does your organisation provide to women?
2. Describe the women's situation in the country or in the community where you work.
3. Are the rights of women recognised? Is equality of women before the law guaranteed? [Probe on the equality of women before law vis-a-vis what is happening on the ground.]
4. Does the state's constitution provide for the equal rights of women?
5. How would you assess your government's compliance with women's rights standards?
6. What are the problems of women in the country/your community?
7. What are the major women's human rights violations? How prevalent are these? How do issues of class, ethnicity, religion, sexual orientation, etc. impact upon women's rights violations generally, and violence against women specifically? What has been done to address these?
8. Does the state recognise VAW and provide for adequate administrative, civil and penal remedies in cases of VAW? What support services are provided?
9. What do you consider some of the more significant improvement/s in the lives (or status) of women in your country in recent years? What about setbacks?
10. How often do you receive reports and cases of violence against women? How about cases of technology-related VAW?
11. What are the common cases of technology-related VAW reported to your organisation?
12. Do you have a profile of the victims/survivors and perpetrators of technology-related VAW? (age, gender, class, disability, gender/sexual orientation, ethnicity)
13. In your assessment or opinion, how distinct or similar is technology-related VAW from/to other forms of VAW? For example, in terms of the effects of technology-related VAW on the victims/survivors?
14. What specific programmes and efforts are being taken by the organisation to address VAW and technology-related VAW?

Do you know of any other organisation or government agency responding to or providing services for technology-related VAW?

15. What problems do you encounter in assisting women victims/survivors of VAW/technology-related VAW?
16. What would facilitate responding to reported cases of technology-related VAW?
17. Considering the current context in the country, what must be done to address VAW? Technology-related VAW?

7. Semi-structured interviews with internet intermediary representatives

Objective: In addition to assessing *availability*, by mapping and identification of corporate policies (complaint procedures, terms of use/codes of conduct, privacy policies, content regulation policies), this research seeks assess the *effectiveness* of implementation of such policies in providing redress to

victims/survivors. Interviews will be conducted with representatives of selected internet and telecommunications corporations, in order to:

- Establish a connection with internet intermediaries, opening a space for dialogue about technology-related VAW and corporate social responsibility.
- Assess internal corporate structure in terms of commitment to gender equality and the possibility of effective implementation of anti-VAW actions.
- Invite input into future research-action design by profiling success stories and fielding possibilities in terms of corporate actions to respond to VAW.

Note: The interview questions below are to guide the interview with the corporate representatives. Familiarising yourself with the questions beforehand will help you shape the interview you conduct so that you have the relevant information needed to assess the adequacy and effectiveness of their practices and policies to provide redress for technology-related VAW, and for upholding human rights and women's rights.

Regarding consent and confidentiality: In the introduction to the interview (sample introduction included below), explain that the interview will be recorded and the findings published as part of the research project. The individual interviewees will not be named, but the corporation itself will be identified by the research.

Considerations on who to approach and how: A key element of obtaining the answers to questions laid out in this interview will depend on what department the representative interviewed works in. Ideally, the interview should be conducted with a representative from user policy departments, or public policy teams. Legal departments at this stage should be out of the scope for interviews. In the desk review of the corporations' policies, country partners will likely uncover the most accessible point of entry.

It may be the case that an initial interview needs to be followed up with another interview with a different representative in another department. As such, where interviewees are unable to provide information on certain questions, ask for the reference and specific contact of someone who might be able to provide that answer. Interviews should be conducted in-person wherever possible. If gaining access to an in-person meeting proves challenging, telephone or Skype interviews are another option, particularly for shorter follow-up interviews for the purpose of clarifying responses.

As explained in the introduction to the interview, the focus of the discussion is on "the role of intermediaries in promoting women's rights" and on "reporting mechanisms, policies and procedures" to promote women's safety.

Interview template

Respondent name:

Position in organisation:

Contact phone:

Contact email:

Introduction

This interview is being conducted as part of an international study by the Association for Progressive Communications on the intersections between technology and violence against women. Our starting point in this research is to examine the availability and effectiveness of the policies and redress mechanisms that ICT corporations have in place to address women's rights violations.

We hope that this project will help build public-private partnerships to prevent technology-related violence against women, and to facilitate women's access to justice. We are inviting your participation as a key stakeholder in the ___(partner country)___ ICT industry.

The interview should take about 45 minutes. It will be recorded, and the research findings will be published in reports exploring women's safety and security in regards to ICTs.

Questions are divided into four sections:

1. Responding to reports of rights violations

1. When a complaint is filed by users in relation to a perceived violation of their rights, what is the internal process for responding and what departments are involved? What policies/guidelines are referred to?
2. What is the usual response time? If it depends on the case, can you provide a few scenarios which would have different response times, and why?
3. How many staff are responsible for responding to complaints?
4. What is the gender makeup of the staff? (How many staff are women, how many are men?)
5. What training do staff receive to fulfil their responsibilities? Does this include gender-sensitivity training? (What is the rationale for this?)

2. Monitoring reports of rights violations

6. Does your organisation keep records of complaints filed by users on rights violations?
7. Please describe the record keeping system, how long records are kept for, which departments are responsible for this data. Please provide links to/soft copies of any policies governing data retention of complaints.
8. How many complaints were received in 2013? 2012? 2011?
9. Are the rights violations organised into specific categories (i.e. privacy violation, human rights abuse, sexual harassment, etc.)? What are the categories?
10. Is the data disaggregated by gender? (i.e. does the organisation record the gender of the user filing the complaint as part of its records?)
11. Please provide gender-disaggregated data on the number of rights violations by category in 2013, 2012, 2011. (If the representative doesn't have access, who in the organisation can provide this data? If the information cannot be shared, why not? Does this violate a policy? Or does the monitoring system simply not exist?)
12. What is the most common type of complaint received? (If they have no data, ask in the representative's opinion.)
13. Does the organisation have a specific reporting system for violence against women?

13.1. If yes, please explain the system.

13.2. If no, what prevents this? (e.g. Doesn't seem relevant? Lack of resources? Lack of expertise? Other?)

14. Is the possibility of developing partnerships with local women's non-governmental organisations (NGOs), grassroots organisations, research centres, and so on for research and/or prevention efforts being explored?

Please briefly describe any current initiatives and their aims/outcomes.

3. Policy design

15. What mechanisms are in place for community stakeholders to provide input into the formulation and revision of corporate policies and practices?

16. There are an increasing number of global initiatives at the international policy level which encourage and highlight the positive strides corporations are taking uphold and promote citizens' rights.

Does your organisation participate in any of these initiatives? Which ones? How often?

17. Is your organisation a member of the UN Global Compact? Is your organisation a signatory to the Women's Empowerment Principles? Why/why not?

18. Are there other declarations/agreements related to respecting users human rights that your organisation supports or is signatory to?

4. Responding to offline violence facilitated by technology

19. What protocols or policies are in place to deal with user complaints/reports of unwanted behaviour that may escalate to physical violence?

20. Under what circumstances does the organisation collaborate with state agencies (such as law enforcement, social service providers, etc.) when dealing with reports of violence?

21. Can you describe instances where the organisation has collaborated with (a) police, (b) courts and law enforcement, (c) social services (shelters, clinics, therapy, etc.), (d) advocacy groups, in relation to rights violations?

22. Technology-related VAW involves: *_(provide brief explanation)_*. Based on this discussion, has the organisation dealt with any incidents of technology-related VAW? How many in 2013?

23. Are there any particular cases that your organisation sees as an important success in your efforts to protect your users' rights?

24. Is there a particular case in which the organisation's intervention helped a woman receive access to justice after she filed a complaint? (i.e. where the intervention helped stop abuse from happening, or helped in the prosecution of perpetrators of violence)

25. We would like to provide you with two examples of technology-related VAW, and ask, in your opinion, what the appropriate response should be.

25.1. Provide a hypothetical example for the corporation that is relevant to their work.

For example, "In one instance, a video has been secretly recorded of a sexual act

between a woman and a man. The people in the video did not consent to being recorded.

The person who created the recording uploads the video onto the internet, through YouTube and Facebook. The video can be traced back to the individual who uploaded it, because of their user account information.”

- 25.2. Ask what the response should be of the various actors involved. (e.g. What in this instance should the response be from (1) the couple, (2) YouTube, (3) Facebook? What should the repercussion be for the individual who took the video, and the individual who uploaded it?)
- 25.3. What role does your company have/can you see for your company in responding to an incident like this?
- 25.4. The second example will be the case study you are exploring, to assess the decisions and actions they made in response to the case.

8. Template for case study write-up

Note: This is the overarching template for case studies – it is a guide. Case studies will be revised and finalised in collaboration with the international research team.

Section V on Corporate Redress Mechanisms will only be relevant for those selected cases where intermediaries were directly implicated and survivors have been interviewed on their interactions with the intermediary.

Case studies should be written with a narrative arc in mind, as these are women’s stories and experiences that are being shared with a greater public. Wherever possible include the direct words and quotes from the interviewees (whether victims/survivors, community members, police, NGOs, lawyers, corporate representatives) to personalise the story, and illustrate and punctuate the setting, context, analysis and lessons learned/recommendations. The voices of victims/survivors is the primary starting point (even if obtained through review of news articles, and not interviews).

- Profile of the Woman Victim/Survivor

This section should provide a description of the situation of the victim/survivor, paying particular attention to her economic, social and political context.

- o Describe the community or the environment where the woman lives, e.g. isolated, remote, or belonging to a particular tribe.
- o Describe what the victim/woman does: student, professional, mother, etc.
- o Describe familial relations e.g. collective decision-makings, communal etc.

Note: Bear in mind how these contextual realities facilitate the woman's access to justice and what they say about women's situation. It should be part of the analysis.

- The Violation Experienced by the Victim/Survivor

This section should describe the violation as narrated and experienced by the woman.

- o Describe also how the incident affected the victim/survivor.
- o Explore her insights and feelings.
- o Explore the harms she experienced.

- o How family relations, social relations, school life, daily life, sexual life, public life, etc. were affected.

Note: There might be different versions about the story and claims; it is important that we put a premium on the woman's own account of the incident. We are after all surfacing the woman's voice.

- The Efforts of the Victim/Survivor to Seek Justice

This section should describe how the victim/survivor sought remedy for the violation she experienced.

- o Describe the actions taken to deal with the violations.
- o Describe the kind of help she sought from different relevant agencies, including internet intermediaries .
- o Describe how the community or other relevant authorities provide help (e.g. help of the members from the national assembly, the investigation, etc.)

- The Processes and Procedures of the Domestic Legal Remedy

This section should describe the legal processes and procedures that the woman went through.

- o Describe the police investigation; describe the attitudes of the police.
- o Identify and describe the laws that were used in the filing of the case; surface why these laws were used.
- o Describe the court process and procedure; surface discriminatory procedures or attitudes.

- The Processes and Procedures of the Corporate Redress Mechanism

This section should describe the reporting process that the woman went through with the implicated internet intermediary.

- o Based on interview with survivor, identify and describe which policies were invoked in reporting the case.
- o Describe the nature and timing of correspondence between the woman and the intermediary.
- o Describe any steps the intermediary took to facilitate access to legal remedy.
- o Based on interviews with corporate representatives and the survivor, identify relevant gaps in both the policies and internal practices that limited the effectiveness of the response.

- Analysis and Critique as to the Available Remedy for the Victim/Survivor

This section should provide discussion and critique as to the available remedy or chosen remedy using the Access to Justice Framework.

- o Account of woman's (lack of) participation in the entire process.
- o Make use of the indicators for analysis (i.e. Access to Justice Framework) to critique/comment on the legal process, and the response by internet intermediaries.
- o Analysis of how technology-related VAW in this case is situated within the broader context of violence against women in the national context (including lens of sexual citizenship).
- o Summarise key lessons learned (by the women themselves) and their recommendations/ideas for improving access to justice.

9. Guidelines for conducting the interview with VAW victim/survivor

Interviewers should be female with experience in handling VAW cases and trained in the techniques as well as question strategy of interviewing VAW victims/survivors.

Note: Being part of or even training in digital storytelling does not mean that a person is then experienced in handling interviews with VAW victims/survivors. It is a very different “process” from interviewing and recording the story of an individual VAW survivor. It is far more intimate and intense and people should have had experience or training in this, especially with how to deal with potential triggering of trauma.

Before the interview

- Familiarise yourself with the case. Study the available materials about the case prior to the actual interview and made the necessary background checks about the situation, victim/survivor, perpetrator etc.
- Conduct a scenario-building exercise on what might happen in the process of the interview. The safety of the victim/survivor and the research team is paramount. Identify the potential risks (if possible come up with a risk assessment check list) for the interviewer, the victim/survivor, the community and others involved in the research and the precautionary measures needed to avoid or reduce them. Particularly for those partners working in a conflict zone or an area with high level of risk, it would be better to have a security plan.
- Do background checks of all people who will not be directly involved in the actual interview e.g. interpreters, drivers, guides, etc. It is necessary to ensure their safety as well.
- Understand the cultural traditions of people in the particular community that the victim/survivor belongs to. Determine the boundaries of what can and cannot be said.
- Discuss all the potential risks identified and precautionary measures in place to all those involved in the research project so that they participate with full and informed consent.
- Prepare as well the victim/survivor prior to the actual interview. Share the details of the research project - its objectives, processes and parties involved - so that the victim/survivor has enough time to decide for herself regarding her participation. Discuss with the victim/survivor the potential safety and security risks for her.
- In choosing the location for the interview, let the victim/survivor decide where will be best for her. Ensure the location is safe, quiet and provides confidentiality for the interview. The victim/survivor should feel free to relocate the interview to a place that may be more safe or convenient for her.
- In scheduling the interview, let the victim/survivor choose a time and date that is best for her. Share with the victim/survivor a time estimate for the interview in advance and stick to it. The victim/survivor should feel free to reschedule the interview to a time that may be more convenient for her.
- Ask the victim/survivor if there are persons she does not want to be present during the interview, so in case that the person shows up you know to stop the interview and reschedule.
- Ask the victim/survivor as well if she wants someone present during the interview for emotional support. The person present should be briefed on the objectives and process too.
- Prepare a comfort kit for the victim/survivor, e.g. tissue and water.

- Identify support options for the victim/survivor such as information on referrals for counselling, medical care, etc.

During the interview

- Introduce yourself to each other and everyone else in the room.
- Establish rapport and build trust with the victim/survivor. Make the victim/survivor comfortable by chatting about other topics beforehand.
- Ensure that you seek the full informed consent of the victim/survivor. Make it clear to the victim/survivor that participation is entirely voluntary and no payment will take place.
- Ensure the privacy and confidentiality of the victim/survivor. Discuss with the victim/survivor that as a general rule her identity shall be confidential in the research. Any identifiable information such as names, addresses, identification numbers, job information, voice recordings and images shall be closely protected. It shall be ensured also that related research activities such as the methods of disseminating findings do not compromise that confidentiality. However, in cases where the woman insists on using her true identity, she shall be given the option to determine what kind of information and details to publish. The research team should be able to explain to the woman the possible consequences of revealing her true identity and shall at the same time ensure her safety.
- Explain to her the research objectives, the interview process and how you plan on using the material. Forewarn the victim/survivor of the nature of the questions that will be asked.
- Inform the victim/survivor that she may decide to withdraw her consent at any time in the course of the interview. Tell the victim/survivor she is free to ask questions and stop answering questions when she wants.
- Inform/encourage the victim/survivor to ask questions during the interview. The interviewer should answer the victim/survivor honestly and to the best of her ability; if she feels that she is not the best person to answer the question, she should refer the victim/survivor to appropriate NGOs or agencies.
- Ask the permission of the victim/survivor if it is okay to record (tape) the interview and/or take down notes of the conversation. Inform the victim/survivor that she has the discretion on what to record or note down.
- Conduct the interview using the research instrument as a guide. Pay attention to what the victim/survivor is saying and to her non-verbal action and adjust the questions accordingly.
- Be conscious of your word choice or language when responding to the victim/survivor. Avoid making comments that imply blaming the victim or implying that they could have prevented, avoided or resisted the incident.
- Do not intentionally ask questions aimed at provoking an emotional response from the victim/survivor or getting her to reveal something she would prefer to keep private.
- Present a non-judgemental and non-biased demeanour. Listen to the victim/survivor actively and with empathy. Use non-verbal clues such as eye contact and nodding your head to show you are listening. Do not show shock or horror at their stories.
- In difficult moments, pause and give the victim/survivor time to compose herself and wait until she is ready to talk. Remind the victim/survivor that she can stop the interview at any time and has the option to continue the interview at another time.

- Be trained to terminate or change the subject of discussion or focus on a less sensitive topic when the interview is interrupted by anyone.
- If you feel the victim/survivor did not answer the question sufficiently or there is an essential detail that is missing in the story, do not be afraid of rephrasing the question and asking it again. However, respect the victim/survivor's limits. Do not push the interviewee.
- Keep your phone or other devices in silent mode so as not to distract the victim/survivor.
- Be aware of the time.

After the interview

- Get the victim/survivor's feedback. Ask the victim/survivor how she feels about the interview and how the interview process was for her.
- Discuss the next steps in the research process, particularly in terms of communication, process, expectation and her involvement. Inform her as well that you may contact her further for follow-up questions and clarificatory questions.
- Exchange contact information so you can stay in touch with each other after the interview. Keep in contact with the victim/survivor to share updates on progress.
- Refer the victim/survivor to appropriate support services when necessary and when the victim/survivor requests it.
- Lastly, it is the responsibility of the research team to ensure the safety and security of the data and information collected from the time the interview ended up to its storage in organisational computers and other storage devices such as portable USBs. Use encryption software (e.g. TrueCrypt) to ensure security of the file. It is also a must that sharing of information and data online should be done using a virtual private network. Follow the Ethical Guidelines and Protocols outlined for this research project.

References

- WITNESS. (2013). *Conducting safe, effective and ethical interviews with survivors of sexual and gender-based violence*. www.scribd.com/doc/159998474/Conducting-Safe-Effective-and-Ethical-Interviews-with-Survivors-of-Sexual-and-Gender-Based-Violence
- UN Women's Virtual Knowledge Centre to End Violence Against Women and Girls. www.endvawnow.org/en/articles/922-key-informant-interviews.html