End violence: Women's rights and safety online

From impunity to justice: Improving corporate policies to end technology-related violence against women

Rima Athar

Association for Progressive Communications (APC)

March 2015

Ministry of Foreign Affairs

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, Democratic Republic of Congo, Kenya, Mexico, Pakistan and the Philippines. For more information visit GenderIT.org and Take Back the Tech!

From impunity to justice: Improving corporate policies to end technology-related violence against women

2015

Project "End violence: Women's rights and safety online"

Research "From impunity to justice: Exploring corporate and legal remedies for technology-related violence against women"

Rima S. Athar (author) is an independent researcher, human rights activist and feminist organiser. She has been working on a variety of international research and advocacy projects to end gender-based violence, exploring the intersections between culture, sexuality, public space and human rights. She holds a bachelor's degree in International Development and Social Studies of Medicine, and a master's in Education and Society from McGill University. Rima was the lead researcher for the "From impunity to justice" research.

Richa Kaul Padte (editor) is a freelance writer and feminist activist. She writes on issues surrounding gender, sexuality and popular culture. She writes at www.richakaulpadte.com and tweets @hirishitalkies.

Katerina Fialova (research coordinator) is coordinating research activities in the APC "End violence: Women's rights and safety online" project. She also works as the GenderIT.org coordinator.

Jan Moolman (project coordinator) is coordinator of the APC "End violence: Women's rights and safety online" project.

Lori Nordstrom (publication production and proofreading) is the publications coordinator at APC.

The research was carried out in collaboration with Carly Nyst and partners located in seven countries: OneWorldSEE in Bosnia and Herzegovina, Colnodo in Colombia, Si Jeunesse Savait in the Democratic Republic of Congo (DRC), the International Association of Women in Radio and Television and KICTANet in Kenya, an APC project associate in Mexico, Bytes for All in Pakistan, and the Foundation for Media Alternatives in the Philippines.

Credit is due to the research advisory team – Anita Gurumurthy from IT for Change, Joy Liddicoat from APC, Avri Doria and Francisco J. Proenza – for their substantive input into the research design, analysis and peer review of the research findings.

Credit is also due to the final reports' peer reviewers: Erika Smith (an APC project associate in Mexico), Aida Mahmutovic (from OneWorldSEE), and Paz Peña (from ONG Derechos Digitales in Chile).

Financial support provided by the Ministry of Foreign Affairs of the Netherlands Funding Leadership and Opportunities for Women (FLOW).

Published by APC
2015

ISBN 978-92-95102-39-2
APC-201503-WRP-R-EN-DIGITAL-230

Table of contents

Section I: Introduction

1. Background to the research

Between April 2013 and June 2014, the Association for Progressive Communications (APC) carried out a multi-country research project entitled "Ending violence: Women's rights and safety online". The project explored the adequacy[1] and effectiveness[2] of domestic legal remedies and corporate policies/redress mechanisms to address the issue of technology-related violence against women (VAW).[3]

The overarching goals of the research were to:

- *Gather evidence to increase understanding of the dynamics of technology-related VAW*, and of what works and what doesn't in the fight against these forms of violence.
- *Develop recommendations for effective evidence-based legal, civic and community-based response strategies* that can be readily adopted by key stakeholders (primarily women, women's rights advocates, public officials, legal professionals and corporate agents) to fight technology-related VAW.

The research was carried out in collaboration with partners located in seven countries: OneWorldSEE in Bosnia and Herzegovina, Colnodo in Colombia, Si Jeunesse Savait in the Democratic Republic of Congo (DRC), the International Association of Women in Radio and Television and KICTANet in Kenya, an APC project associate in Mexico, Bytes for All in Pakistan, and the Foundation for Media Alternatives in the Philippines.

This report shares the results that directly focus on the availability and effectiveness of corporate policies in facilitating women's and girls' access to justice when they experience gender-based violence – including sexual harassment, sexualised abuse, stalking, threats, coercion, blackmail and/or extortion – through the use of ICT services.

[1]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.

[2]The element of effectiveness includes a) competent, impartial, independent and gender-sensitive legal systems and duty bearers, b) women's active participation in the process, c) speedy and immediate enforcement, d) the existence of immediate protective measures, and e) the existence of monitoring oversight on the part of state or private sector actors to further facilitate and improve women's access to justice.

[3]The UN Declaration on the Elimination of All Forms of Violence Against Women (DEVAW) defines violence against women 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" (see the full text at www.un.org/documents/ga/res/48/a48r104.htm). Technology-related VAW encompasses acts of gender-based violence that are committed, abetted or aggravated, in part or fully, by the use of information communication technologies (ICTs).

1.1 Research method

The research method was three-fold:

- Research teams first documented in-depth case studies on women's and girls' experiences of technology-related VAW, and their attempts to access justice either through domestic legal remedies or by reporting the violation to corporate grievance mechanisms. A total of *24 case studies were documented* across the seven countries.
- Teams then reviewed the corporate policies[4] of the internet intermediaries implicated in the case studies, or those with a large share of the national market. Each review highlighted provisions that could technically allow for the identification, reporting and rectification of instances of harassment or violence against women via the service that the intermediary provides. *The policies of 22 companies were reviewed*.
- Teams also sought *interviews with public policy representatives* of the same internet intermediaries, to (a) gain insight into the effectiveness of their implementation of policies and redress mechanisms in responding to VAW, and (b) document creative initiatives that companies have undertaken to promote awareness on gender, sexuality, VAW and human rights.

1.2 Analytical framework

The analysis of the availability and effectiveness of corporate policies in this research is guided by the Access to Justice framework[5] developed by the Women's Legal and Human Rights Bureau – Philippines (WLB) as well as the UN Guiding Principles on Business and Human Rights.[6]

Access to Justice takes a holistic approach to the concept of justice and remedy. When applied to corporate policy frameworks, it seeks to look beyond the mere presence of policies that clearly address VAW, towards the mores and social norms surrounding their implementation as well as perceptions regarding women's human rights and their bodily integrity. Access to Justice also sees women as active agents and therefore best placed to identify their own strengths and needs. This report specifically responds to women's experiences and their subsequent demands for accountability as demonstrated by the research.

The UN Guiding Principles on Business and Human Rights enshrine a framework of obligations entitled "Protect, Respect and Remedy", which outlines companies' requirements under international law to respect human rights, to avoid infringing human rights, and to address adverse human rights impacts with which they are involved. This means not only do companies have to take action when they play a role in human rights violations, but they must also take positive steps to prevent, mitigate and remedy human rights violations.

Bringing these frameworks together, one output of the research was the creation of a *checklist of key questions/indicators* that organisations, advocates and activists can use to analyse the

[4]The reviews focused on terms of service and privacy policies.

[5]www.ohchr.org/Documents/HRBodies/CEDAW/AccesstoJustice/WomensLegalAndHumanRightsBureau.pdf

[6]www.ohchr.org/Documents/Publications/GuidingPrinciplesBusinessHR_EN.pdf

compliance of internet intermediaries with the UN Guiding Principles, specifically with a focus on preventing VAW (see Annex 1).[7] These indicators frame the discussions within this report.

2. Companies reviewed

Research teams reviewed the policies of the following companies:

Social media and networking platforms	**National telephony companies (telephone, mobile phone, internet services)**	**Search engines and portals**	**Pornography websites**
Facebook Twitter Google+ YouTube Instagram WordPress	Bosnia and Herzegovina: BH Telecom Colombia: Claro, Empresa de Telecomunicaciones de Bogotá (ETB) DRC: AirTel Kenya: Safaricom Mexico: TelCel, IUSACell, Prodigy Pakistan: Pakistan Telecommunications Company Ltd. (PTCL) Philippines: Smart Communications Inc. (SMART), Global Telecommunications Inc., and Philippines Long Distance Telephone Co. (PLDT)	Google, Colombia Microsoft (Bing/MSN Messenger, Colombia Yahoo!, Philippines	Xvideos YouPorn

Note: For simplicity we have categorised the companies in relation to the primary services they provide. The Pakistan research team also reviewed the policies of the Pakistan Telecommunications Authority (PTA) for the potential of industry regulatory mechanisms to address technology-related VAW.

This report does not aim to present an in-depth exploration of each or any one company's policies and practices, nor does it make an extensive comparative analysis across companies. Rather, this report *summarises some of the common obstacles to resolving technology-related VAW within current corporate policy frameworks* and uses individual examples of company policies in order to shed light on best practices or possible solutions that respond to women's demands for corporate accountability.

It is important to note that despite research teams' repeated attempts to contact companies, most companies were not willing to participate in the research or discuss the topic publicly.

[7] APC. (2014). Internet intermediaries and violence against women online: User policies and redress frameworks of Facebook, Twitter and YouTube. www.genderit.org/node/4076

Out of 22 companies, only six gave interviews.[8] This report therefore presents the data that was available to research teams, while noting that the companies surveyed here may be taking other steps that are not publicised.

3. Report structure

The following discussions should be seen as a starting point in a longer, ongoing conversation, given that the scope of corporate actions in upholding human rights will continue to change and be shaped by rapid technological advances (e.g. in access, connectivity, design and infrastructure) as well as emerging laws and standards regulating ICT companies internationally and locally. Though focused on areas for innovation regarding corporate social responsibility (CSR), the discussions do not suggest that strategies to address technology-related VAW depend solely on advocacy towards ICT companies, nor that corporations as private actors can or should mediate access to justice outside the purview of international and domestic law. Domestic legal remedies (the presence of relevant and effective laws, public policy forums, law enforcement and digital forensic services, anti-VAW support services, etc.) are primary avenues for access to justice for women and girls who fall victim to technology-related VAW. APC's research report on domestic legal remedies is available separately.[9]

Following this introduction, *Section II: Trends and tensions within corporate policy frameworks* explores three categories of companies: national telephony companies, social media and networking platforms, and pornography websites. Each sub-section (a) provides a snapshot of the violations documented in the research, and (b) discusses possible steps to address technology-related VAW for companies.
Section III: Exploring legal liability discusses the role that liability has played in shaping company policies and practices. It also highlights liability measures that have been introduced in recent laws addressing technology-related VAW.

Section IV: Business and human rights summarises various guidelines at the international level and highlights how companies reviewed here have approached these in their practices.
Section IV: Summary and recommendations concludes the report with a short recap of insights for (a) individuals seeking recourse through ICT companies, (b) anti-VAW advocates, and (c) areas for further research.

[8]Interviews were held with AirTel (DRC), BH Telecom (Bosnia and Herzegovina), ETB (Colombia), Google-Colombia, Microsoft-Colombia, and YouTube.

[9]Women's Legal and Human Rights Bureau, Inc. (2015). *From impunity to justice: Domestic legal remedies for cases of technology-related violence against women.* APC. www.genderit.org/VAWonline-research

Section II: Trends and tensions within corporate policy frameworks

1. National telephony companies

Research teams reviewed the policies of the following companies: BH Telecom, Claro, Empresa de Telecomunicaciones de Bogotá (ETB), AirTel, Safaricom, TelCel, IUSACell, Pakistan Telecommunications Company Ltd. (PTCL), Smart Communications Inc. (SMART), Global Telecommunications Inc., and Philippines Long Distance Telephone Co. The Pakistan research team also reviewed the policies of the Pakistan Telecommunications Authority (PTA) for the potential of industry regulatory mechanisms to address technology-related VAW.

1.1 Summary of violations

Within the research, mobile phones were the most commonly used tool to perpetrate technology-related VAW. Mobile phones allowed aggressors to maintain an abusive relationship and inflict psychological and emotional violence on women and girls when physical contact was not possible. While in a few cases unknown aggressors engaged in harassment and intimidation through calls or SMS, in the majority of cases involving mobile phones, *the harassment and intimidation that women faced was located within the context of (ongoing) physical abuse from a known aggressor*. The extended violence that women faced fell into categories of domestic violence, intimate partner abuse, homophobic violence, kidnapping, rape and sexual assault. While recognising that state services and law enforcement are primarily responsible for enabling women's access to justice in addressing such violence, the research also provided insights into the roles that companies can play to help provide avenues for redress.

1.2 Steps to address technology-related VAW[10]

1. Provide clear and specific definitions of unlawful, illegal and abusive behaviour, particularly forms of technology-related VAW, within terms of service (ToS).

Terms of service (ToS) are the most direct form of agreement between a company and a user. They outline the contractual obligations of both parties, including the general environment and terms of engagement that companies would like their services to enable. Within the ToS, companies generally have clauses outlining users' responsibilities to refrain from "unlawful", "illegal", "fraudulent", or "abusive" behaviour while using their services. But in most cases *the ToS provide no depth as to what constitutes illegal and/or abusive behaviour.* Perhaps the lack of definition for "illegal" and "unlawful" behaviour indicates a catch-all that encompasses such behaviours as defined by national laws. However, the lack of definitional clarity in written ToS

[10]National telephony companies provide a multitude of services, including internet access, email, DSL land line telephones, prepaid and post-paid phone services, cloud hosting, and more. Most companies have individual ToS for each element of their service provision (see for example Safaricom's "other services" at www.safaricom.co.ke/about-us/about-safaricom/terms-conditions/other-terms-conditions). For the purposes of this research, teams reviewed the general ToS, or those specifically for pre- and post-paid phone services.

leaves individuals without a clear understanding as to what kinds of behaviours they can report should they be subjected to abuse by other users. Within this research, for example, women and girls from Bosnia and Herzegovina (Vanessa, Rebecca), Colombia (Alejandra, Antonia, Irene), DRC (Tatiana), Kenya (Beatrice, Che), and Mexico (Louisa, Mary),[11] all received threats of physical and/or sexual violence through mobile phones. Yet *no national telephony company reviewed here names threats of physical or sexual violence as prohibited behaviour*. A strong policy statement that provides specific examples of what constitutes unlawful, illegal or abusive behaviour – such a threats of physical or sexual violence – would be an important first step in creating a more responsive environment to technology-related VAW. However, while a policy statement is an initial step, even a strongly worded ToS is rendered useless if not accompanied by (a) a clause detailing what actions may be taken when the terms are violated, (b) information directing users to multiple accessible reporting mechanisms (e.g. reporting options via web, phone, email and in person), and (c) clear disclosure of the procedures – how and when such complaints are monitored and processed.

2. Detail within the ToS exactly what action will be taken when illegal and/or abusive behaviour occurs through use of services.

Detailed reporting mechanism

A prominent gap in the ToS reviewed here is that not all companies have a clear section of their ToS which details what steps a user can take to report actions they feel are a violation of (a) the ToS, (b) their own rights and/or (c) another users' rights. A transparent process would ensure that ToS clearly and simply detail *what complaint mechanisms exist, how these mechanisms can be availed of, what information users will need to provide to the company, and the expected medium and timeline of response users can expect.*

Claro (Colombia) provides a positive example in this regard. In its website ToS, it highlights that anyone seeking to make a complaint of any sort (malpractice, unlawful use of services, abusive content, intellectual property rights) should contact the company as follows:[12]

> For these purposes, the affected party or claimant should send a notification to CLARO containing the following information: (i) Personal information: name, address, telephone number and email address of the affected party or claimant; (ii) a precise description of the supposedly illicit or improper activity or practice carried out on the portal or through the services provided and/or marketed by CLARO, and in particular, in the case of a supposed violation of rights, a precise and concrete description of the protected contents as well as their location on the pages of the CLARO portal and/or website; (iii) facts or circumstances that demonstrate the improper or illicit nature of the practice; (iv) an express and clear statement under the responsibility of the claimant that the information

[11] See: www.genderit.org/node/4221

[12] English translation of Claro Términos y Condiciones, Section 12 www.claro.com.co/wps/portal/co/pc/personas/legal-y-regulatorio?1dmy&urile=wcm%3apath%3a/claro2013.colombia/pc/personas/legal-y-regulatorio/lightbox-fijo/terminos-y-condiciones

provided to CLARO is correct and true. (v) When the practice reported by the claimant may constitute criminal conduct, CLARO will inform the competent authorities of the facts reported in the notification provided by the claimant.

Disruption of services

While the level of detail provided by Claro was not matched by any other company reviewed here, most other companies' ToS did have a clause pertaining to a "disruption of services". This clause allows companies to reserve the right to suspend or terminate access to services, with or without notice, if a user is found to be in breach of the ToS, particularly in regards to a user's financial liability and/or engaging in "illegal" behaviour.

Of the companies reviewed, Safaricom's prepaid phone services[13] offered one of the strongest examples in relation to technology-related VAW:

5. SUSPENSION AND DISCONNECTION OF SERVICES

(a) We may suspend (bar), restrict or terminate the provision of the Services (in whole or in part) without informing you and without any liability whatsoever (although, we will, where possible, try to inform you that such action is or may be taken) under the following circumstances:

i. If we are aware or have reason to believe that your Equipment or SIM card is being used in an unauthorised, unlawful, or fraudulent manner (or has been so used previously) or if you choose not to use the Services for a period of over one hundred and twenty (120) days after the end of the validity of your last Re-charge).

iii. If you do not comply with any of the conditions relating to any part of the Services;

iv. If we believe you are making calls or sending data which is classified in our sole opinion as being illegal, a nuisance, abusive, a hoax, menacing or indecent (including any calls or messages relayed to our customer service operators).

From the standpoint of its potential power, Safaricom's policy has provisions wide enough to cover various forms of technology-related VAW. This could include threats, harassment, intimidation, extortion and blackmail – carried out via calls, SMS, MMS, or other data transfer. The policy is explicit in describing the actions it may take as a result. It also technically provides enough room to put an immediate stop to the abuse if and when it is reported.

[13]Safaricom Prepay Terms & Conditions, Section 5
www.safaricom.co.ke/images/Downloads/Terms_and_Conditions/conditions_of_use_for_the_safaricom_prepaid_services.pdf

However the lack of a clear definition of what the company considers "*in its sole opinion* as being illegal, a nuisance, abusive, a hoax, menacing or indecent" again *leaves users without clear guidelines on what behaviours they can report, and moreover grants the company seemingly arbitrary and excessive power in determining when to terminate an account or even to take a report seriously*. The lack of transparency or accountability of company decisions in this regard presents an obstacle to ensuring due process and effective responses to reports of abuse, both for those filing complaints and those accused of offences.

It should also be noted that the standard "disruption of services" clause appears to primarily ensure companies' rights to suspend services when they are owed monies for said services; there is little evidence that even companies who do list abusive behaviour as reason for suspending or disconnecting accounts actually use this option for recourse when users are reported as being abusive. Within the research, when women who were being threatened or harassed did contact phone companies asking for help, they were told there was little to nothing the company could do – despite pertinent clauses in their ToS.

In order for such a policy to provide effective redress, the following factors would need to be considered:

- The judgement being in the "sole opinion" of the company requires *a dedicated team of staff to record and investigate complaints* of illegal or abusive behaviour in a formal and timely manner, above and beyond a general "customer service" department. The details of these kinds of departments (what records they keep, what kinds of reports they receive and with what frequency, whether they have enough staff for the volume of complaints, and what transparency measures are in place regarding company decisions on complaints) were key questions this research sought to answer. However, no companies surveyed demonstrated any formal public records for such details.
- *Where domestic laws do not perceive threats, particularly via telephone or SMS, as unlawful or illegal actions, women and girls may be left without recourse.* In one case study, a woman living in a city in Republika Srpska (Bosnia and Herzegovina) attempted to file a complaint with the police due to threats of violence she was continuously receiving via SMS from an abusive ex-partner over a period of two months. The police said that since threats through SMS were not unlawful, they could not take any action against the aggressor.[14] In another case, a woman who lives in Mexico State (Mexico) tried to report death threats she received via SMS and email to the police. The police informed her that because threats are not criminalised in Mexico State, they would take no action.[15] *Normative biases in laws that minimise threats against women often turn into corporate policies that do the same*. This is one area where telephone companies could create internal policies and practices in line with their responsibilities under the UN Guiding Principles, perhaps through a *disruption of services for repeated offences*.
- Even if companies enact their disruption of services policy in regards to complaints of stalking, harassment and threats through a transparent and accountable process, it could be argued that disconnecting the service of an aggressor entails a short-term

[14]See: www.genderit.org/node/4235

[15]Threats are criminalised in the legislation of other states of Mexico, therefore individuals seeking recourse in other jurisdictions may have recourse. See: www.genderit.org/node/4238

solution in the case of technology-related VAW. Multiple concerns come into play: simply disabling an account, especially if the user is notified as to the reason, does not stop the aggressor from switching companies or SIM cards and continuing to harass the survivor. Moreover, in cases of violence against women there is often a precedent for not providing detailed notice to an aggressor to avoid retributive action against a victim/survivor. A commitment to providing redress for women and girls involves *addressing the immediate needs of the victim/survivor in accordance with her consent*. These needs may include seeking information about choices for formal legal recourse, medical help, counselling, blocking the abuser, obtaining an alternate SIM card, etc. Such a commitment requires *providing adequate training of company staff to understand the dynamics of how telephony services are being used to perpetrate VAW*.

3. Provide full and clear disclosure on the processes accompanying companies' legal obligations and voluntary commitments to track, monitor, block and record part of or all user communications and personal information of users.

Formal logging and reporting systems on user data

All companies are governed by the national legislation of the country within which they are incorporated and/or operate. According to the national laws in place, each company may be obliged to intervene, block, track, record or request information about a user and their account for the purposes of law enforcement, mostly when mandated by the appropriate authority.

While all companies are bound by such legislation, few state exactly what they will monitor as explicitly as Safaricom (Kenya):[16]

> You accept that we may disclose and/or receive and/or record any details of your use of the Services including but not limited to your calls, emails, SMS's, data, your personal information or documents obtained from you for the purposes below: [followed by a list of purposes]

TelCel (Mexico) also explicitly mentions the tracking of geographic location, in accordance with Mexico's recently passed "geolocation law":[17] [18]

> In accordance with the current regulations, the COMPANY may, with no responsibility on its part: (i) be prevented from providing or continuing to provide

[16]Safaricom PrePay Terms and Services, Section 2.g. www.safaricom.co.ke/images/Downloads/Terms_and_Conditions/conditions_of_use_for_the_safaricom_prepaid_services.pdf

[17]English translation of TelCel Términos y Condiciones. www.internet.telcel.com/terminos-condiciones.html

[18]The newly passed law on geolocation introduces measures that would allow a public prosecutor's office to use written or electronic requests directed to Mexican mobile phone operators to request the location of a mobile phone *without the need of a judge's permission*. Once the public prosecutor's office has located the phone, the public prosecutor's office would need a warrant signed by a judge to tap the calls, to call for a search warrant for the site of the phone, or to arrest the person who is carrying it.

> services; and further (ii) be obliged to provide information relating to the communications and geographic location of the CUSTOMER.

PLDT (Philippines) suggests they may voluntarily provide information to law enforcement, particularly in emergency circumstances:[19]

> We may also use or disclose your personal information if required to do so by law or in the good-faith belief that such action is necessary to (a) conform to applicable law or comply with legal process served on us or the Website; (b) protect and defend our rights or property, the Web site or our users, and (c) act under emergency circumstances to protect our safety and security and those of our affiliates, agents and the users of the Web site or the public in general.

Companies should provide greater transparency within their privacy policies and ToS in regards to exactly what content and data use they can and will track; what they may be obliged to hand over to law enforcement in accordance with which laws; and in what instances they may voluntarily accede to law enforcement or state services. Lack of transparency obscures the fact that extensive, detailed reporting mechanisms can and do exist, and that voluntary cooperation with law enforcement may take place beyond court orders for certain emergency situations. It also *obscures the ways in which such systems and processes could be developed further to help provide redress in cases of technology-related VAW and other human rights violations*.

Formal requirements for disclosing personal information to law enforcement

Standard procedures across countries and companies surveyed require that in order for companies to cooperate with law enforcement, (a) a court order, subpoena, or warrant must first be obtained by affirmation of a judge, (b) then provided to the company by the appropriate authority (a specific public ministry or police department) and delivered through official reporting mechanisms, and (c) examined and confirmed by the company's legal department before the company takes any action to disclose appropriate data. If requests are too broad, companies may seek to narrow the scope; this, however, results in prolonged negotiations in court and other legal channels.

Despite the bureaucracy involved and the length of time it adds to processing complaints, requiring a court order before companies disclose users' personal data provides a system of checks and balances that limits abuse of privacy rights by governments, state authorities, companies and individuals. Divulging personal identifying information at random to a complainant constitutes a clear violation of privacy, whereas the requirement of a court warrant or another official requisition form creates a system preventing infringement on due process, or the violation of the privacy rights and security of users.[20]

[19]Philippines Long Distance Telephone Co., Privacy Policy. www.pldt.com/privacy-policy

[20]As with the example of Mexico's law on geolocation, standard procedures differ across national contexts in terms of the levels of cooperation expected by companies according to the laws in place.

4. Invest in educational tools and resources to inform users about their rights and responsibilities.

A lack of clear and accessible information fuels legal illiteracy amongst technology users. APC's research has documented that a lack of awareness and understanding of legal systems is one of the main obstacles to women and girls accessing justice, particularly in relation to technology-related VAW. While ToS usually mention the national jurisdiction that governs the contract, and privacy policies may mention specific consumer protection laws they abide by, a case can be made for companies to *develop more highly visible and easily accessible legal information for users*.

Claro and ETB (Colombia) were two companies out of those reviewed that provided "User Guidelines" beyond the ToS. These guidelines detail which laws impose specific liability on each company, as well as any ministry regulations and guidelines the companies follow. Claro, for example, details its compliance with User Protection Communications Resolution 3066/2011; Habeas Data Law 1581/2012 and Decree 1377/2013; and Law 679 of 2001 regarding child pornography. ETB includes the same laws and also references Act 1336 of 2009 and Decree 1524 of 2002 in relation to child pornography.

Providing a **one-stop "legal awareness centre**" with simple language that details which laws and provisions govern which corporate policies, and even provide links to soft-copies of the laws, would help users to:

- Navigate the *intricacies of privacy laws, consumer rights laws, ICT laws, etc.* that directly impact their rights and responsibilities.
- Be informed in writing of *the requirements for law enforcement* to request information from companies, and have access to these forms themselves.
- Be informed of the *concrete steps, reporting and communication patterns, and timelines for action that the legal department takes* in relation to specific requests.
- Be directed to appropriate *resources and services in cases where companies take no responsibility* in addressing a rights violation (e.g. providing links to anti-VAW advocacy groups, women's shelters, police centres, hotlines for bullying and suicide prevention, etc.).

It is also important for multinational enterprises to *detail the particular jurisdictions that govern the parent company and its subsidiaries*, so users availing of grievance mechanisms know which legally incorporated entity they will actually be engaging with. To ensure ease of access this information could take the form of a centralised and prominently displayed portal on companies' websites.

In an interview, ETB (Colombia) also highlighted their investment in other kinds of "safety and security" education, prevention and response initiatives as a key strength of their approach to curbing technology-related violence. ETB has developed 61 interactive web portals to educate users on safety and security on the internet and through mobile communications. ETB is also

allied with the national "Te Protejo" ("I Protect You") programme,[21] which is dedicated to raising awareness and facilitating reports of child abuse, exploitation and trafficking.[22]

5. Develop transparent and accountable systems to stop harassment via telephony services.

Within the research, women who were facing harassment sought to block numbers from contacting them. Company policies and interviews have confirmed that each company can and does have internal records of the date and time of each incoming and outgoing call or SMS, which number it was to and from, as well as the location from which it was sent. Standard operating procedures require these records to ensure appropriate billing for services. With such data available, there is ample room for companies to *implement redress systems to prevent/block contact between users*. However, among the companies reviewed, BH Telecom (Bosnia and Herzegovina) appears to be the only one with such a mechanism in place.

BH Telecom's policy is that if a customer receives unwanted phone calls from a number four or more times within 24 hours, BH Telecom may investigate by calling the harassing user and warning them that they are in breach of the terms of use, after which point BH Telecom may offer recourse in the form of blocking the contact. The presence of this policy is refreshing, but the experience of Vanessa demonstrated that the policy's effectiveness is fraught with limitations: Vanessa believed that her stalker was very likely aware of the policy, because he never called more than three times in a 24-hour period. Instead, he would call one or two times, and then again two times in the next 24 hours, and so on. Despite clear evidence of repeated harassment, BH Telecom said it could not investigate the case since it did not fall within its policy guidelines.[23]

BH Telecom's response demonstrates a need for greater training and awareness around the nature of stalking and abuse, and how to develop policies that could adequately respond to such situations. If an aggressor continues to change numbers with each phone call, there may be little a company can do. But if certain phone numbers consistently show up in records (e.g. for a week or over the course of a month), a proactive approach could be taken. It is also important to flag here, however, the need to develop redress mechanisms that include a system of checks and balances on company investigations and decisions to prevent the exercise of arbitrary censorship. *Company decisions should be detailed in writing and recorded with an independent formal authority* (e.g. with cyber crime units or commissions on digital violations). Even if the company's decisions are not made available to the general public, registering with a formal authority increases transparency for the basis of the company's investigation, judgement and actions vis-à-vis users' rights.

[21] www.teprotejo.org/index.php/es

[22] Colnodo. (2014) Interview with ETB representative. Transcript on file. Unpublished.

[23] See: www.genderit.org/node/4235

6. Build upon existing proactive and cooperative programmes that exist in cases of child sexual exploitation, trafficking and kidnapping.

One case study from Mexico involved the kidnapping and forced sexual servitude of three girls, who were all minors at the time. The aggressor targeted the girls by first flirting with them, and then exercising psychological and emotional blackmail and threats via SMS to coerce them into obeying his orders. One girl, Mary, escaped and reported the incident to the police, and the police issued a warrant for the accused's arrest. However, when the aggressor fled to an unknown location, the police did not take any initiative to work with his telephone service provider to track him or to find the other missing girls. A social worker interviewed in the case believes the lack of action on the part of the police was due largely to attitudes that tacitly accept VAW.[24]

Mary's case raises the question of how telephony companies can facilitate access to justice through programmes against child exploitation and trafficking, especially where discriminatory attitudes within the police may present an obstacle to reports being taken seriously.

In an interview, BH Telecom (Bosnia and Herzegovina) highlighted its steps to build formal relationships with state agencies, law enforcement and international services that bring greater attention to the issue and encourage faster action on child exploitation. Under the initiative of the State Ministry of Security, BH Telecom participated in developing an industry-wide action plan (2010-2012) to improve protection systems against child pornography and other kinds of sexual exploitation through ICTs. In practice, BH Telecom still requires a court order or warrant to intercept traffic, but the company plays an active role in facilitating quick action. When there are reports made of child exploitation through the services, BH Telecom will alert the police, who will then apply for the court order to log the information. This differs from the more common procedure that requires individuals to report to the police, who then have to accept and file the claim, and only then proceed to take investigative action.[25]

While these types of programmes offer a possible avenue for recourse, further information is needed on the strengths and accessibility of such initiatives.

7. Ensure that industry or company guidelines address specific forms of violence, and are accompanied by appropriate training for staff on technology-related VAW.

Where individual companies prove reluctant to develop such policies, lobbying could be directed towards national regulatory authorities to set standards that compel companies towards social responsibility.

The Pakistan Telecommunications Authority (PTA) provides an example in its guidelines on "Protection from Spam, Unsolicited, Fraudulent and Obnoxious Communication Regulations, 2009".[26] The PTA guidelines define "obnoxious communication" as "the transmission of message/statement with the intent to cause harassment or disturbance". Clause 10 of the

[24]See: www.genderit.org/node/4238

[25]OneWorldSEE. (2013). Interview with BH Telecom representatives. Transcript on file. Unpublished

[26]Cited in: Bytes for All Pakistan. (2014). *Violence Against Women – a review of the policies of ICT intermediaries in Pakistan*. Unpublished.

document requires that "all Operators must set up a standard operating procedure to ensure that all possible technical solutions are available to the subscribers in a transparent and non-discriminatory manner to control obnoxious communication." The PTA guidelines also outline specific mechanisms to handle complaints, as outlined below:[27]

- Recording of all telephone numbers including area code (where applicable) of a complainant.
- Telephone number and area code (where applicable) of the originator of the obnoxious communication.
- Issuance of warning immediately but not later than 24 hours of receipt of complaint and recording the same in the grey list being maintained by the operator.
- If the originator is repeatedly involved in obnoxious communication even after issuance of warning, the operator shall terminate the outgoing communication of the telephone subscription of the originator immediately but not later than 24 hours of the receipt of the complaint.

Technically, guidelines such as these could provide a framework for dealing with hate and abuse received through SMS and calls; however, they would only be effective *if the specific forms of violence were named, and clear examples and definitions provided*. For example, instead of catch-all terms (such as "obnoxious communication" or "abusive behaviour"), specific acts of violence should be named (such as "harassment or hate speech on the basis of gender" or "verbal and/or written threats of physical or sexual violence").

Once an appropriate policy guideline is in place, regulatory agencies may also have reporting or grievance mechanisms that could be used to demand accountability from ICT companies.

For example, the PTA website prominently features a "Complaints" section,[28] where it offers (a) contact details (phone numbers, emails and addresses of in-person service centres) of each national telecommunications provider to facilitate users filing complaints directly with their providers, (b) contact details for the offices of the Consumer Protection Directorate (CPD), useful in cases where users have filed complaints with their telecommunications providers and are unhappy with the results, and (c) multiple methods of filing a complaint through the PTA directly, including a call centre helpline, fax, post, email and web form to lodge a complaint.

[27]Pakistan Telecommunications Authority. (2009). Protection from Spam, Unsolicited, Fraudulent and Obnoxious Communication Regulations, Section 11.4. www.pta.gov.pk/media/pro_spam_reg_09.pdf

[28]www.pta.gov.pk/index.php?option=com_content&view=article&id=1589&Itemid=770

8. Engage more deeply with women's experiences, immediate needs, and demands for accountability vis-à-vis technology-related VAW.

When researchers asked company representatives from AirTel (DRC),[29] BH Telecom (Bosnia Herzegovina),[30] and ETB (Colombia)[31] how their companies would and could respond to technology-related VAW, representatives' responses centred on three main points:

- That law enforcement is responsible for addressing VAW
- That a court order is essential to protect privacy rights
- That women and girls should take steps to keep themselves safe.

Without denying the validity of these points, framing the debate solely in these terms limits any nuanced and creative discussion on the topic. It equates internet intermediaries' responsibilities solely with their legal obligations – concepts that need to be separated – and places the onus squarely on state services and individuals to end VAW. It also presumes that the only demand by women seeking redress for technology-related VAW is identifying harassing users, and *obscures the possibility of coming up with more holistic solutions to technology-related VAW*.

[29]Si Jeunesse Savait. (2014) Interview with AirTel representative. Transcript on file. Unpublished.

[30]OneWorldSEE. (2013). Interview with BH Telecom representatives. Transcript on file. Unpublished.

[31]Colnodo. (2014). Interview with ETB representative. Transcript on file. Unpublished.

2. Social media and networking platforms

Research teams reviewed the policies of the following social media and networking companies: Facebook, Google+, Instagram, Twitter, WordPress, and YouTube.

2.1 Summary of violations

Social media platforms have come under higher scrutiny and public pressure to address technology-related VAW due to the ways they enable communication and sharing of information at unprecedented speeds and without borders. This has made acts of violence harder to contain and also created new challenges for prosecution and access to justice. Within the research, violations committed through social networking platforms centred on:

- Creation of "imposter" profiles of women, often to discredit, defame and damage their reputations.
- Spreading private and/or sexually explicit photos/videos, often with intent to harm, and accompanied by blackmail.
- Pages, comments or posts targeting women with gender-based hate (including misogynistic slurs, death threats, threats of sexual violence, etc.).
- Publishing personal identifying information about women including names, addresses, phone numbers and email addresses without their consent.

Interestingly, most of the companies reviewed do have mechanisms in place that should technically respond to the above violations. However, it is impossible to assess the effectiveness of these mechanisms due to the fact that *little to no public information is available about how internal review processes work*. This includes how complaints are dealt with, what the ratio of complaint handlers to the volume of complaints is, what kinds of training on gender, sexuality, law and human rights the staff receives, the time limits for the review process, and clear policies on whether complaints are brought to law enforcement and under what circumstances. In addition to a lack of transparency on internal decision-making processes, *no social media/networking company surveyed had made a public commitment to human rights*, nor demonstrated a clear understanding of violence against women. Some steps, however, have been taken.

2.2 Steps to address technology-related VAW[32]

1. Recognise the importance of social context in formulating content-regulation and privacy policies, particularly in regards to VAW.

[32]Note: To the extent that some trends overlap with telephony companies, this section has omitted those considerations (e.g. cooperating with law enforcement, legal literacy, expedited cooperation on child pornography, etc.), focusing directly on trends and tensions unique to social media and networking platforms.

APC's research explored the policies of Facebook, Twitter and YouTube in detail,[33] including analysing the steps the companies have taken in response to controversial content. In three prominent cases – concerning (a) nudity, (b) gender-based hate, and (c) the normalisation/tolerance of graphic violence – the controversy has centred precisely on *these companies failing to uphold women's rights and denounce violence against women*. As a result of public demands for accountability from individual users, civil society and women's rights groups, the companies have been forced to review their policies and delve deeper into exactly *what values they are promoting with their terms of service and community standards*. Slowly companies are recognising the need to examine the social context of VAW to be able to better respond to the issue.

Differentiating nudity from "obscenity", sexually explicit content, and/or pornography

A tension that arises when companies put a blanket prohibition on "nudity" is that they tend to uncritically equate the naked physical body with obscenity, sexually explicit material, and pornography. A human rights-based approach to corporate policies would ensure that the terms of service, community standards and privacy policies do not inadvertently censor consensual sexual expression, nor contribute to a conservative mindset that reduces women's bodies to sex objects. Yet this is often what happens. A simple example is the way in which women's nude breasts and nipples are often deemed "obscene", and become the subject of content takedowns, while nude male chests and nipples are not. *Such a policy arbitrarily restricts women's freedom of expression and their rights to bodily autonomy.*

Facebook has been at the centre of demands by women to change its policy to ensure women are not silenced or degraded. It has recently changed its Community Standards around "Nudity and Pornography" to take social context into account and separate the two concepts. Its policy states:

> Facebook has a strict policy against the sharing of pornographic content and any explicit sexual content where a minor is involved. We also impose limitations on the display of nudity. We aspire to respect people's right to share content of personal importance, whether those are photos of a sculpture like Michelangelo's David or family photos of a child breastfeeding.

Recognising that gender-based hate is not simply "offensive" or "humorous"

Between 2012 and 2013, Facebook and Twitter both came under intense public pressure for failing to take any action on content that promoted, glorified, or threatened women directly with rape, sexual assault and physical violence.[34] [35] The initial reaction and inaction of these companies in deference to "free speech" and "humour" demonstrates an inadequate

[33]APC. (2014). *Internet intermediaries and violence against women online: User policies and redress framework of Facebook, Twitter and YouTube.* www.genderit.org/node/4076

[34]Gayomali, C. (2013, 29 May). Facebook's disgusting hate speech problem. *The Week.* theweek.com/article/index/244815/facebooks-disgusting-hate-speech-problem

[35]Gayomali, C. (2013, 29 July). Why Twitter doesn't punish people who make rape threats. *The Week.* theweek.com/article/index/247513/why-twitter-doesnt-punish-people-who-make-rape-threats

understanding of hate speech and VAW, and effectively condones both. It also fails to recognise the severity of psychological and emotional impacts of VAW. It was only after large public campaigns condemning the companies' inaction, and advertisers threatening to drop their spots, that they took any public stance on the issue. Facebook issued a single apology and statement that it would update its training to address gender-based hate, and Twitter brought in new reporting and blocking mechanisms for its users. While these are positive steps, it remains to be seen how effective these changes will be, especially without any *transparency on what trainings on gender, VAW, laws and human rights are being provided to content-reviewers at these companies*.

Normalisation/tolerance of graphic violence

In May 2013, a video circulated on Facebook that showed a masked man slitting the throat of a woman and then beheading her. One of Facebook's Safety Advisory Committee members objected to the content as inappropriate – particularly for younger users – and public outcry caused Facebook to place a temporary ban on graphic violence until it reviewed its policy. On 21 October 2013, the company's revised policy continued to allow graphic images, but stated that content review teams would "take a more holistic look at the context surrounding a violent image or video, and [would] remove content that celebrates violence." It would, however, still allow videos "of public interest or concern".[36] With this decision Facebook initially allowed the video of the woman being murdered to come back online. It was only with more public demands for accountability that Facebook removed the video permanently, as it failed to qualify how this constituted a video of "public interest".

Facebook's approach to "gratuitous violence" is troublesome. While it is important that the company saw the need to look at the context around the video and the intent with which it was shared on the site, the content itself was not publicly recognised or denounced by Facebook as a form of violence against women. The shift from banning "graphic violence" to banning "gratuitous violence" also begs the question of what forms of graphic violence companies see as acceptable. The sharing of videos and photos of graphic violence showing crimes (e.g. murder, executions, torture, sexual violence) must be systematically reviewed by social media/networking companies. APC has previously noted how *the sharing of such videos often re-victimises the women and girls featured*, who have to relive the trauma of their assault with each share.[37]

YouTube's policies provide users with perhaps the most guidance as to what constitutes unacceptable portrayals of violence and inappropriate content. YouTube explains that "It's not okay to post violent or gory content that's primarily intended to be shocking, sensational or disrespectful," and states that "if your video asks others to commit an act of violence or threatens people with serious acts of violence, it will be removed from the site."[38] Parts of the

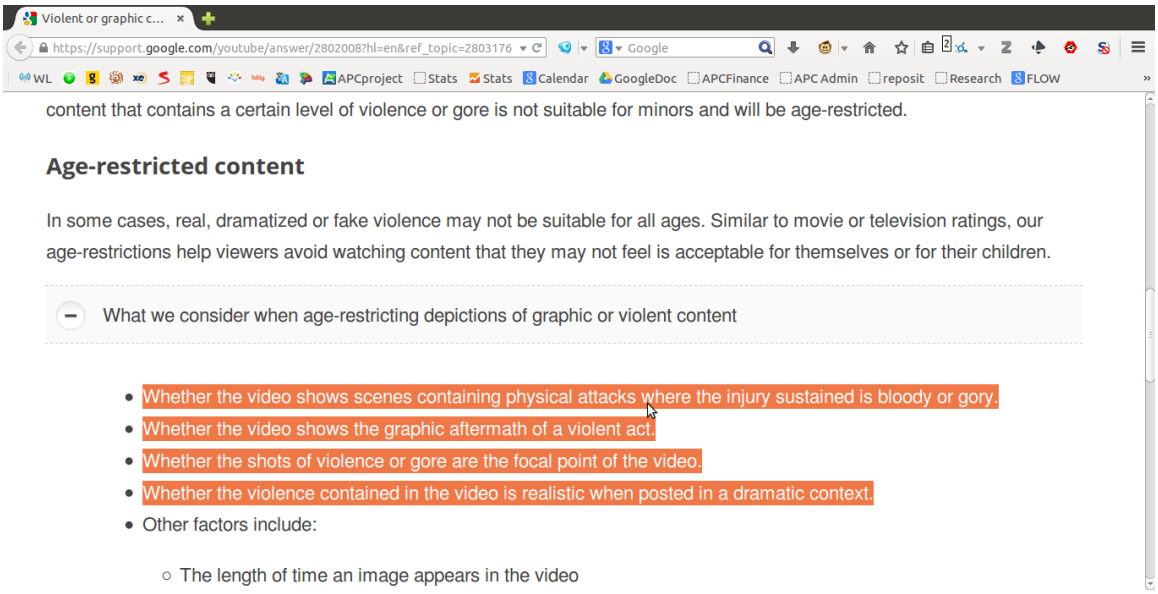
[36]Harrison, V. (2013, 23 October). Outrage erupts over Facebook's decision on graphic videos. *CNN Money*. money.cnn.com/2013/10/22/news/companies/facebook-violent-videos

[37]Fialova, K., & Fascendini, F. (2011). *Voices from Digital Spaces: Technology-related violence against women.* APC. www.genderit.org/node/3539

[38]support.google.com/youtube/answer/2801964?hl=en&ref_topic=2803176

policy also detail the kinds of cues content reviewers will look for when seeking to age-restrict a video. Pertinent clauses include:[39]

- Whether the video shows scenes containing physical attacks where the injury sustained is bloody or gory.
- Whether the video shows the graphic aftermath of a violent act.
- Whether the shots of violence or gore are the focal point of the video.
- Whether the violence contained in the video is realistic when posted in a dramatic context.



YouTube's policy on hate speech also prohibits hate on the basis of gender, among other identity markers. Overall the policy presents an example of heightened transparency and responsibility towards users regarding violent and abusive content, and creates the space to provide redress for certain forms of technology-related VAW.

2. Strictly prohibit the publishing of private, confidential, and/or identifying information of others.

Clearly defining "private" and "public" information

Among the companies surveyed there exists a discrepancy in how strongly they condemn the distribution of private, confidential and/or identifying information. While ToS often prohibit users from publishing identification documents, financial information, credit card numbers, social security numbers, unlisted telephone numbers, complete addresses and private email addresses, they also state that full names and publicly available information are not prohibited. However, *it is unclear what constitutes "publicly available" information* – whether this is determined according to particular laws and jurisdiction on official public records, or

[39] support.google.com/youtube/answer/2802008?hl=en&ref_topic=2803176

whether information available anywhere on the internet is deemed public and therefore can be re-posted at will. The lack of clarity raises questions for users' safety and security. For example, if an address of a private citizen is available on the internet, does that automatically qualify it as "publicly available"? Is the question of how that information was distributed to begin with taken into account? Where does a user's consent to release personal information enter the equation? Companies genuinely concerned with privacy should make user profiles completely "private" as the default setting, encouraging users to make informed and individual decisions about what information they choose to share and make public. Yet the trend is the opposite, and increasing personal data in the public realm can present heightened safety risks for individuals.

These tensions are exemplified by the case of Baaghi, a woman human rights defender from Pakistan.[40] In the context of years of online hate and abuse, Baaghi was alerted to a blog that had published her national identity card, the application form for the card, her marriage certificate, her educational certificates, her family's photographs and the addresses of all the places she had lived during the previous 10 years. These details were posted alongside a call for her and her family to be killed. One month later there was an assassination attempt on her life. In her interview, Baaghi did not suggest a direct causal link between the two actions, but she does continue to live in fear that further attacks will be made on her and her family at their homes, especially given the viral spread of information and continued attacks. She says: "I had nightmares all the time of being raped by these bastards, of them doing harm to my parents, my husband and my daughter because of me. I still get nightmares that they have done something to my daughter, or kidnapped my husband."[41]

Policies should be explicit as to what constitutes "public" and "private" information, and ensure minimal obstacles to taking down pages, pictures, comments, posts, etc. in relation to privacy concerns – especially when information is accompanied by threats and incitement to violence. Where companies refuse to take down such content, there should be a clear accountability measure in place to at minimum provide a detailed written response for the decision to the complainant, referencing the exact policies and laws being followed.

3. Address the English language bias in reporting mechanisms.

While the largest platforms – Google+, YouTube and Facebook – do make the majority of their policies available in over 40 languages, it is unclear whether the actual reporting forms are available across languages. It is also completely unclear to what extent the staff responsible for processing takedown requests are multilingual. This presents acute challenges for non-English speaking women who try to report privacy or content violations.

In one case study, Serena from Sarajevo (Bosnia and Herzegovina) was alerted to a fake and slanderous Facebook profile created to damage her reputation. It was not until she received

[40]See: www.genderit.org/node/4239

[41]Ibid.

help from OneWorldSEE that she was able to report the profile to Facebook; the reporting forms were all in English, a language Serena does not speak.[42]

In the case of Baaghi (Pakistan), numerous fake profiles were created of her on both Facebook and Twitter. She recounts her attempt to report to Twitter:

> I had to use that feature of Twitter where they take you to a page where you have to fill in the whole form and filling in the whole form takes 20 to 30 minutes. Once you've sent the form, they write back to you asking you to submit your ID card copy, which should be in English. Our ID cards are in Urdu. So either you get a translated ID card issued (an arduous task) or send a copy of your passport, which is in English. Essentially, Twitter requires any government-issued picture ID in English.

While Baaghi could present an English language passport, the demand to submit an English-language government issued ID card to verify identity presents a serious obstacle for women and girls attempting to access justice while living in non-English speaking countries. Baaghi also faced obstacles trying to report hate and abuse to Facebook, as the content she was trying to report was in Urdu script:

> I reported many, many times. They want to know what kind of abuse it was, whether it was racial, ethnic or sexual in nature. Once you have pinpointed then they ask what exactly was said. Now how would they understand what was said if it's in Urdu or Punjabi? So if I cut and copy the text, for example, the word "motherfucker" in Punjabi, how would they know it's "motherfucker"? You don't have the option to type the translation, you have to paste the phrase that was used, so one has to paste the exact phrase and they don't know what it is.[43]

Companies with such an international reach have *a basic responsibility to make privacy and content reporting mechanisms accessible to all users*, ensuring that the forms are available in national languages, and that multilingual complaint handlers are employed to review such complaints.

4. Promote mutual legal assistance treaty (MLAT) reform to increase access to justice in cases of technology-related VAW.[44]

Mutual legal assistance treaties (MLATs) are the primary means through which US-based companies cooperate with law enforcement in other countries, particularly around criminal investigations. That these treaties are a cumbersome bureaucratic process is widely

[42]See: www.genderit.org/node/4235

[43]Bytes for All Pakistan. (2014). *Case study number 2, Pakistan.* Unpublished.

[44]See, for example, Google's informative video on the process at googleblog.blogspot.ca/2014/03/transparency-report-requests-for-user.html and www.youtube.com/watch?v=MeKKHxcJfh0

acknowledged, and MLAT reform is a dialogue that many internet intermediaries are part of. However, until this system improves, there appears to be little option for efficient recourse for users in countries apart from the United States. Most companies do have an option for "emergency disclosure" requests, but it is unclear whether and under what circumstances law enforcement from other countries can access this. Companies should provide greater transparency in this regard.

5. Provide greater transparency and accountability regarding (in)action on content and privacy requests.

In multiple case studies, women reported either a total lack of response, or an automated response from companies that did not detail a timeline for action, what action - if any - was taken, and why (or why not) content was removed.

In one case study, Vanessa from Goražde (Bosnia and Herzegovina) was stalked and harassed for years by a former romantic interest. One of his moves was to upload a video to YouTube, in which he used her Facebook photos, identified her by name, and detailed the city in which she lived. According to Vanessa: "If someone who did not know the entire story saw it, they would probably think that it is a sweet love story. However, I was going through a horror story. As soon as I saw the video, I immediately ran to take pills to calm my nerves down."[45]

When Vanessa reported the video to YouTube, the company did not respond to her request. This inaction was despite YouTube's reporting form, which suggests that personal images and full legal names being shown *do* constitute privacy violations.[46]

While materials may be flagged inappropriately and may not actually violate ToS, such *a lack of clear communication mechanisms is inadequate in guaranteeing transparency and accountability that reports are being taken seriously or addressed at all*.

Baaghi (Pakistan) recounts the isolating effect this can have on users who are being bombarded with hate and abuse online:

> The least these companies could do was interact with me at that point in time and assure me. I understand that anyone can make ghost complaints, but there should be mechanisms for assessing your complaint. I, being a victim, should be understood by these managements. After assessing the complaint, they should actually be interacting with the complainant to assure her of any concrete action they would be taking. The whole mechanism should be made easy for the complainant, not add piles and piles of work and burden on the complainant who is already under pressure and depression. Also, the least Twitter could have done was to offer me a verified account,[47] obviating the need for hundreds of

[45]See: www.genderit.org/node/4235

[46]YouTube's policy on Privacy Violations can be found here https://support.google.com/youtube/answer/2801895?hl=en and the reporting form is available here https://support.google.com/youtube/contact/privacy2

[47]Twitter verifies accounts to make it easier for users to find who they're looking for. However, verified accounts are only meant for "highly sought users in music, acting, fashion, government, politics, religion,

complaints related to abusive fake (impersonation) accounts in my name, which were using my picture and bio data.[48]

6. Provide greater transparency and public accountability about the departments and staff responsible for responding to content and privacy complaints.

There is little to no information available publicly about (a) the number of staff/teams dealing with complaints, (b) the languages they speak, (c) what training is provided on gender, sexuality, VAW, law and human rights, or (d) where the teams are located. Facebook presents a positive example by providing an infographic and a webpage explaining "What Happens When You Report Something".[49] But even this still stops short of providing exact details.

7. Reserve the right to terminate accounts specifically on the basis of repeated gender-based harassment, hate and abuse.

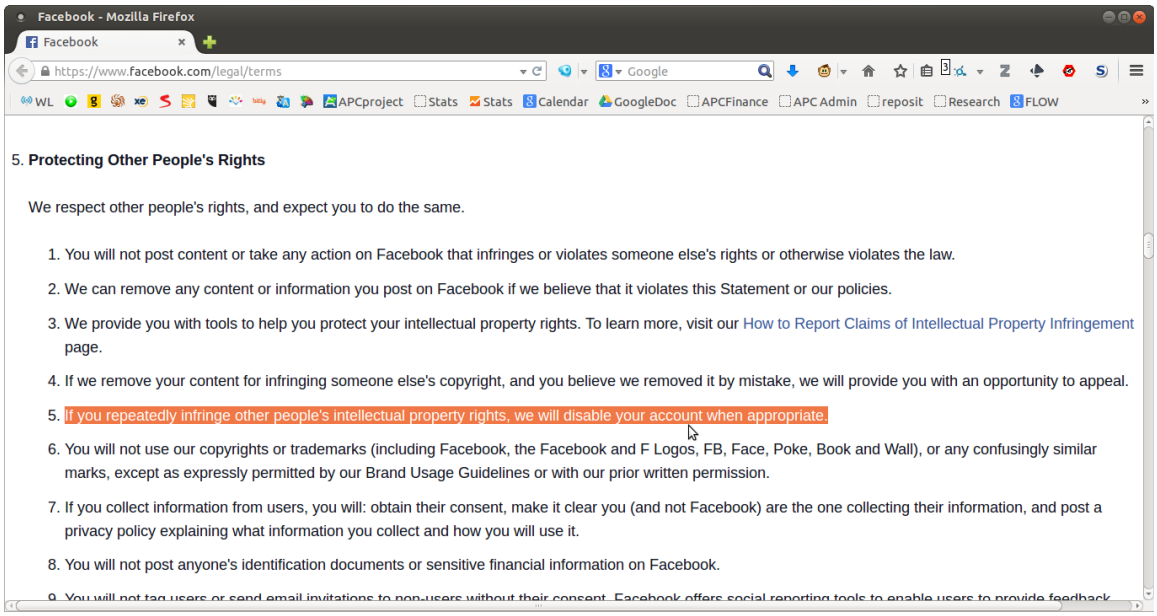
Similar to other internet intermediaries, social media and networking platforms often have a standard disclaimer allowing them to terminate a user account, either with or without notice, should the account be in violation of any of the ToS. But as with other intermediaries, protecting intellectual property rights appears to be the main priority for social media companies.

journalism, media, advertising, business, and other key interest areas." Twitter says it does not accept requests for verification from the general public. See https://support.twitter.com/groups/31-twitter-basics/topics/111-features/articles/119135-about-verified-accounts#

[48]Bytes for All Pakistan. (2014). *Case study number 2, Pakistan.* Unpublished.

[49]facebook.com/notes/432670926753695

For example, in Facebook's policy on "Protecting Other People's Rights",[50] out of all the possible violations of users' rights, account suspension is only mentioned as a consequence in relation to copyright infringement. Facebook states that it will provide users with tools to protect intellectual property rights, and the policy links directly to information on how to report this violation:

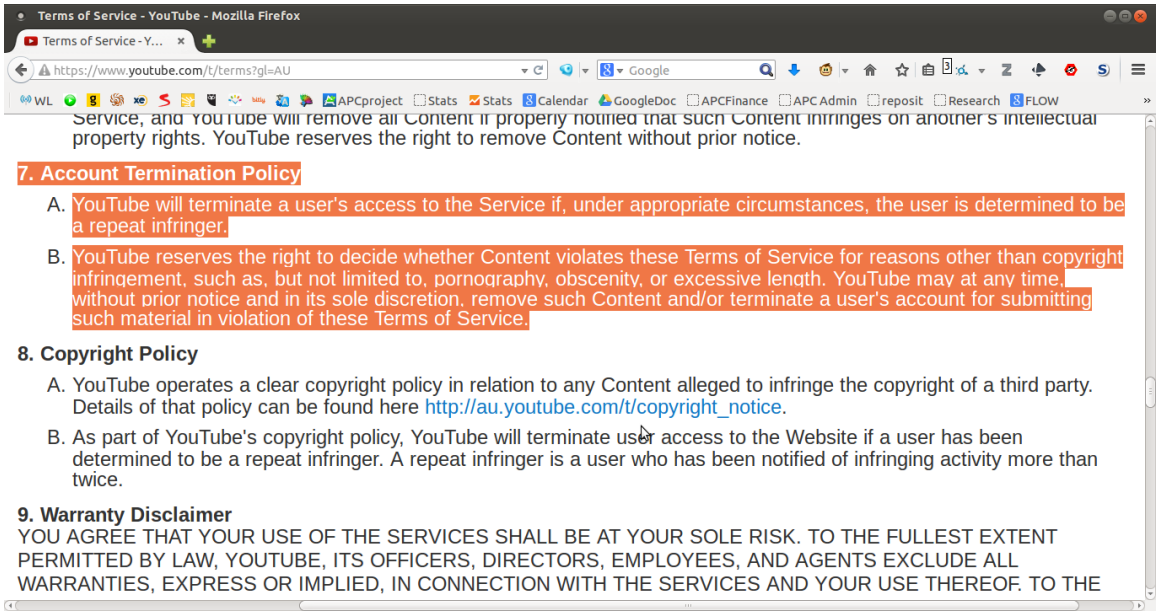


While YouTube's "Account Termination" policy[51] states other concerns, it still lacks a clear stance on hate, abuse, violence and privacy violations:

> **A.** YouTube will terminate a user's access to the Service if, under appropriate circumstances, the user is determined to be a repeat infringer.
>
> **B.** YouTube reserves the right to decide whether Content violates these Terms of Service for reasons other than copyright infringement, such as, but not limited to, pornography, obscenity, or excessive length. YouTube may at any time, without prior notice and in its sole discretion, remove such Content and/or terminate a user's account for submitting such material in violation of these Terms of Service.

[50] www.facebook.com/legal/terms

[51] www.youtube.com/static?template=terms



Multiple strike policies should be expanded beyond copyright concerns and implemented for accounts that repeatedly infringe others rights to privacy, security and bodily autonomy more broadly: whether they repeatedly harass, intimidate and/or abuse others, repeatedly create pages that get flagged and removed, or repeatedly post private information (including photos, videos or identifying information).

8. Ensure system-wide removal of individual content (photos, videos, tweets) at source.

All companies collect the metadata surrounding each piece of uploaded content. Metadata refers to technical details that help describe how, when and by whom a piece of user content was uploaded and how that content is formatted. When it comes to photos and videos being uploaded and spread virally, metadata should enable companies to track and trace content and its spread across their entire platform, and therefore ensure its takedown across an entire platform as well. While YouTube has a system to remove a video at its source, it is unclear whether the same mechanism is in place on Facebook, Twitter or Instagram, to name a few. *Companies should show greater transparency in this regard, and move towards a clear system that enables this platform-wide removal system, including posts that have been shared, re-posted, re-tweeted, etc. by other users*.

9. Engage with experts in gender, sexuality and human rights to provide input into policy formation, staff training, and the development of education/prevention programmes.

Facebook provides another positive example through its Safety Advisory Board, comprised of five prominent internet safety organisations. In collaboration with the US National Network to End Domestic Violence, Facebook released "Safety and Privacy: A Guide for Survivors of

Abuse"[52] in July 2013. Facebook also has a Network of Support comprising five US-based LGBT advocacy organisations, and has commissioned research for its "Compassion Project", which looks into bullying and harassment online. Such moves demonstrate a willingness and effort to learn from civil society on how to address rights issues. However, this engagement should be expanded to groups outside of North America and the European Union to better address the needs of users in other regions who actually make up the majority of Facebook users. Guides and research should also be made available in multiple languages to benefit the widest possible number of non-English-speaking users.

3. Pornography websites[53]

The responsibility of pornography sites as intermediaries in response to technology-related VAW appears to have received less public attention than other kinds of intermediaries, despite the likelihood of such platforms being used to distribute videos and photos taken without the consent of the people featured.

3.1 Summary of violations

The research documented one case study involving pornography sites. Berenice, a schoolteacher from Mexico in her early 30s, was alerted by friends to the existence of a video on a pornography site featuring her having sex. In an interview she recounted:

> When I saw [the video], I knew it was me, I recognised my blanket and my bed and I was wearing one of my blouses. But in the second part where I appear without a blouse, I realised, "That's not my body, my arms are chubbier and back then I had long hair. In the video, I was just talking but when I stop talking, the montage part of the video starts, where the other girl's body appears.

Berenice's face had been morphed onto the other woman's body, and the title of the video also mentioned the town where Berenice was from. Before Berenice knew about the video, she had an experience that she now connects to the existence of the images online. She recalls:

> A few months ago, two guys, each one on a different day, approached me. I was coming from school and one guy stopped me and began to talk to me, saying that he knew an intimate part of my body – my breasts – and that I was a whore for showing them and that he treated whores like me very badly. … I told him that I

[52] www.facebook.com/notes/facebook-safety/safety-and-privacy-on-facebook-a-guide-for-survivors-of-abuse/601205259900260.

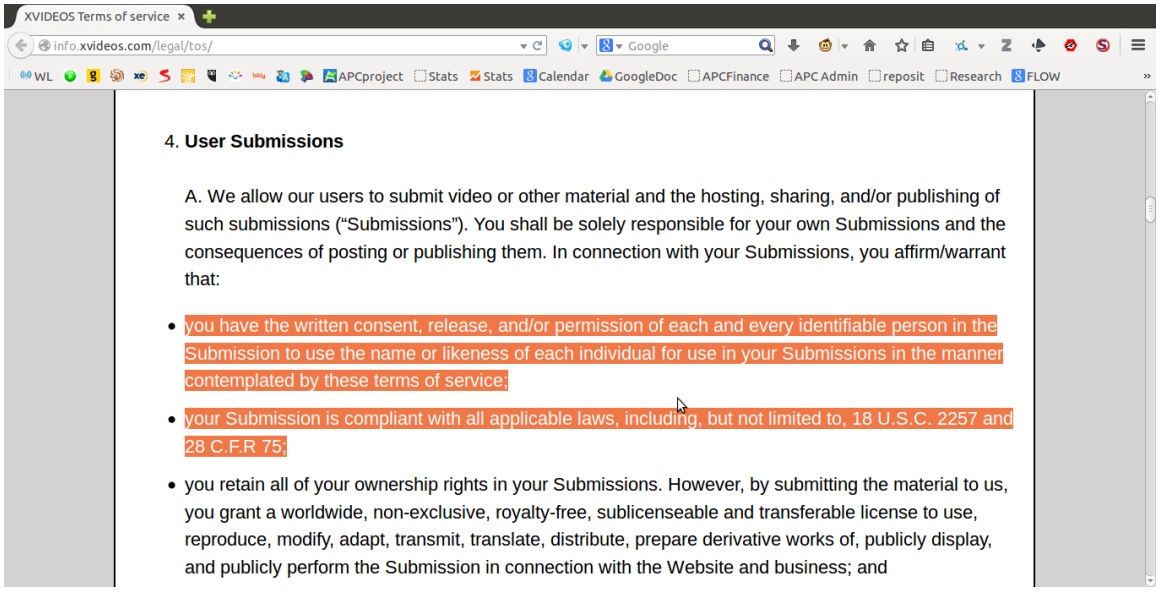
[53] This research does not equate pornography websites with what - in the US especially - have come to be termed "revenge porn" sites. From a rights-based approach, this research regards "revenge porn" as a misnomer that obscures the underlying violence embedded in the act of distributing intimate and private photos/videos without the consent of the person featured. In simplified terms, we see pornography as sexually explicit content, filmed, edited, produced and distributed with the free and full consent of all parties involved. By contrast, this research takes the filming, editing, production and distribution of sexually explicit content without full and free consent of all parties involved, and/or with intent to harm, as an act of aggression and an abuse of individuals' rights to privacy, security and bodily autonomy.

> was going to tell the police, although there weren't any police officers on the street where I was walking, but I saw a store so I went in to buy something and the guy disappeared.[54]

Berenice's friend reported the video to one pornography site, Xvideos. "When he reported the video, they asked him for a reason, why he was reporting it. 'It's my sister,' he said. The company explained to him that everything that is uploaded to that page is protected." Regardless, the video was taken down. While the company did not explain why, its action suggests that it may have recognised it as a violation of its policies in the end. Other companies, however, did not remove the video, with no communication as to what terms or policies they were following nor an explanation of why this did not qualify as a violation.

3.2 Steps to address technology-related VAW

The ToS of XVideos reveals a number of strong provisions that should afford remedy in cases of technology-related VAW. Particularly, the terms regarding "User Submissions":[55]



> We allow our users to submit video or other material and the hosting, sharing, and/or publishing of such submissions ("Submissions"). You shall be solely responsible for your own Submissions and the consequences of posting or publishing them. In connection with your Submissions, you affirm/warrant that:
>
> - you have the written consent, release, and/or permission of each and every identifiable person in the Submission to use the name or likeness of each individual for use in your Submissions in the manner contemplated by these terms of service;

[54]See: www.genderit.org/node/4238

[55]Note: This link will connect you directly to the XVideos website: info.xvideos.com/legal/tos/ Section 4.

- your Submission is compliant with all applicable laws, including, but not limited to, 18 U.S.C. 2257 and 28 C.F.R 75;[56]

- you retain all of your ownership rights in your Submissions. However, by submitting the material to us, you grant a worldwide, non-exclusive, royalty-free, sublicenseable and transferable license to use, reproduce, modify, adapt, transmit, translate, distribute, prepare derivative works of, publicly display, and publicly perform the Submission in connection with the Website and business; and

- the posting of your Submission on or through the Website does not violate the privacy rights, publicity rights, copyrights, contract rights or any other rights of any person; and

- you agree to pay for all royalties, fees, and any other monies owing any person by reason of any Submissions posted by you to or through the Website;

The strength here is that the terms clearly establish the responsibility of the uploaders to prove that they had the written consent, release and/or permission of each person featured. The terms highlight an explicit respect of privacy rights, and suggest users are responsible for any civil lawsuits arising from their submissions. XVideos' ToS also directly link to "Reporting Forms" to flag any violations of the ToS, yet the reporting mechanisms demonstrate the weaknesses in terms of providing actual redress for technology-related VAW.

No recognition of other forms of privacy violations or abuse within reporting mechanisms

The most prominent reporting mechanism is for copyright infringement, particularly with respect to US law. Within this form, there exists a detailed description of the company's actions in regards to content takedown on the basis of copyright infringement. The company has a dedicated team, method and timelines of response, and a clear system in place to deal with such complaints. For all other reports of violations on XVideos there exists one general form with no explicit description of the communication a reportee can expect, whether they will be notified at all, and/or what other forms of recourse they may have if their request for a takedown is refused by the company. There is one menu option to report "inappropriate content", which suggests inadequate recognition of the different kinds of rights violations that take place and an inadequate record keeping system.

[56] 18 U.S.C. 2257 is the US Federal "Child Protection and Obscenity Enforcement Act", and 28 C.F.R. 75 refers to the guidelines for enforcing the law, and in particular, mandates strict record keeping by producers on the ages of all actors/models involved in sexually explicit photos/videos.

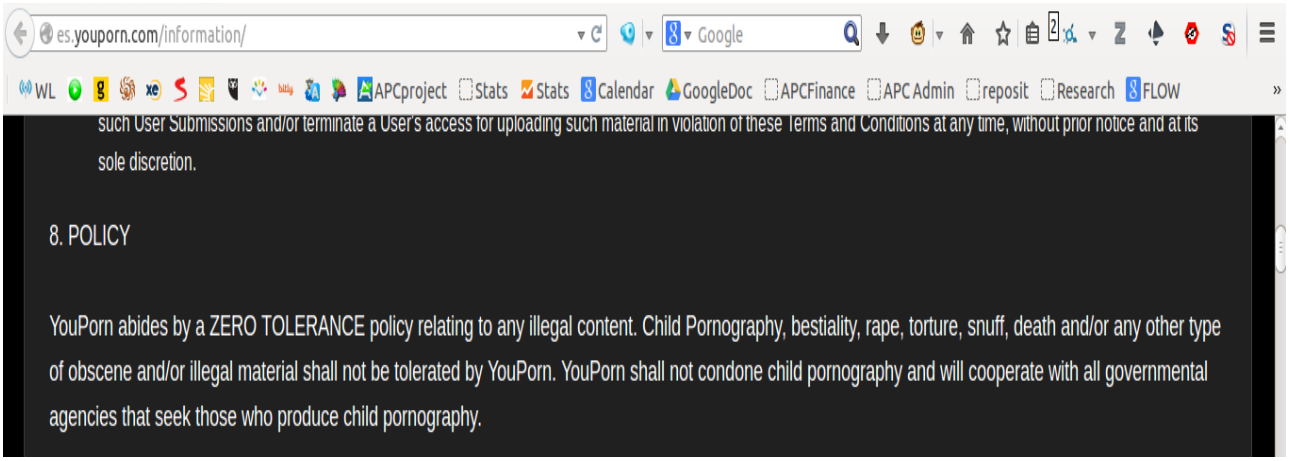
Unclear where burden of proof lies when reporting abuse

Without a detailed explanation of decision-making procedures, it remains unclear how XVideos applies its policy regarding written consent, and with whom the burden of proof lies. The research would advocate that the user who uploaded the submission should have to produce evidence that they have the written consent/release, rather than the complainant having to prove otherwise.

No mechanism to suspend accounts when terms are violated beyond copyright

When Berenice tried to report the account of the user who submitted the video – whose profile constantly boasted of uploading stolen videos and photos of women and underage girls – XVideos stated that the profile was protected content and would not examine the account. According to its policies, the only way an account gets suspended is by "3 Strikes on Copyright Infringement".[57] XVideos' policy on account suspension is in stark contrast to another site, YouPorn.

YouPorn's ToS present a detailed policy on reasons for terminating accounts should users abuse the service, particularly on hate crimes, pornography, and obscene or defamatory material. YouPorn also clarifies what it means by "illegal content": [58]



> YouPorn abides by a ZERO TOLERANCE policy relating to any illegal content. Child pornography, bestiality, rape, torture, snuff, death and/or any other type of obscene and/or illegal material shall not be tolerated by YouPorn. YouPorn shall not condone child pornography and will cooperate with all governmental agencies that seek those who produce child pornography.

[57]Note: the following link will connect you directly to the XVideos website: info.xvideos.com/legal/repeat/

[58]Note: the following link will connect you directly to the YouPorn website: es.youporn.com/information/

A cursory look at the ToS of other large internet pornography sites suggests similar rules regarding submissions, prohibited content and takedown policies. Given the nature of the content, the terms appear to set a strong policy framework for responding to technology-related VAW, particularly the distribution of videos of sexual assault and/or rape, as well as the unauthorised and non-consensual distribution of private intimate or sexual photos and videos. Or as in the case of Berenice, image manipulation to feature a person without their consent. However, the adequacy and effectiveness of the actual takedown procedures of these sites remains unknown, especially without further documentation or evidence of people's attempts to contact companies in cases such as this. The fact that the video of Berenice was not removed from many pornography sites and can still be found online indicates a clear lack of attention and interest in dealing with and addressing technology-related VAW by many service providers. Based on the experience of Berenice, a number of clear steps can be taken to improve pornography sites' responsiveness:

- *Create a dedicated contact form specifically for the purpose of "reporting abuse"*, with detailed reasons (e.g. divulged personal identifying information, filmed without consent, uploaded without consent, rape/sexual assault), and *develop consistent and detailed procedures for responding to content takedown requests* through this form (such as a timeline for action, counter-claims, etc., in as much detail as procedures for copyright infringement).
- *Create multiple strikes "account suspension" policies explicitly for users who repeatedly upload materials in violation of the ToS and the privacy rights of others*, including disseminating videos/photos without the explicit consent of all individuals featured.
- *Ensure that when a video is flagged/reported as one distributed without consent, the burden of proof lies with the submitting/uploading user* to demonstrate that they obtained the consent of all parties in any videos they uploaded, rather than placing the burden of proof on the survivor.
- *Ensure a system-wide removal of content*. In other words, once a video is taken down, the removal must be consistent across the original website, no matter who else has shared it, and thereby also removed from pornography aggregator sites.
- *Within the ToS make clear exactly which court jurisdiction applies to the ToS and user actions.*
- *Clarify exactly when and how a site will cooperate with law enforcement, both nationally and internationally*.

Section III: Exploring legal liability

While this research supports the idea of limiting liability on internet intermediaries regarding third party content in the same way that concepts of transparency, privacy and accountability need to be enlarged in the debate on technology-related VAW, perhaps a more nuanced look at liability is also necessary.

The original design of this research noted that "internet intermediary liability can occur around issues such as: copyright 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."[59]

After reviewing company policies, it becomes evident that the standards across *the ToS of many internet intermediaries are primarily reflections of their legal obligations, and not much more than that*. A look at legal liability also sheds light on why, for example, certain issues get explicit attention from corporations in their written policies and redress mechanisms (such as copyright infringement, child exploitation, financial fraud and extortion), but others do not (including violence against women, gender-based hate and other human rights violations). When looking for avenues for prevention and redress in relation to technology-related VAW, *there appears to be growing recognition across countries that certain levels of liability are warranted and necessary to protect and respect women's rights*.

When APC began its work on technology-related VAW in 2011, there was little to no public recognition of the issue. In the last four years, however, more women have been speaking out about their experiences, particularly regarding the following types of violence:

- Taking and distributing photos and videos of rape and sexual assault, or the threat to distribute such videos.
- Taking, uploading and distributing private photos of a sexual or intimate nature without the consent of the person pictured, often accompanied with identifying information about the person. In many cases, the people pictured are subjected to blackmail and extortion in order to remove these photos.
- Misogynistic hate speech, including threats of death and/or sexualised violence spread through social media, blogs, comment sections on various pages, instant messages, and emails.

With the rise in reporting and visibility, there has also been an accompanying trend towards implementing legislation that can adequately address the issue. In the most unfortunate cases, legislation has and continues to spring up when technology-related VAW leads to the suicide of young girls. In other cases, legislation has been amended in recognition of the failure of existing anti-VAW laws to account for the emotional and psychological impacts of certain types of technology-related violence. Within the timeframe of this research project,

[59]Athar, R., & and Women's Legal and Human Rights Bureau. (2014). *Research Design: Building Women's Access to Justice: Legal Remedies and Technology-related Violence Against Women.* APC. Unpublished.

Israel,[60] Singapore,[61] Brazil, eight US states,[62] and one Australian state all passed laws in this regard.

As part of its broader End Violence research project, APC analysed four such laws in depth:

- The South African Protection from Harassment Act 2010
- The Nova Scotia (Canada) Cyber Safety Act 2013
- The California (United States) SB 255 Electronic Communication Devices: Prohibited Distribution of Personal Information
- The New Zealand Harmful Digital Communications Bill 2013.

The full report on legislative trends is available separately, although some highlights on internet intermediary liability bear replication here:

> The South African, Nova Scotian and New Zealand legislation all reflect the increasing need for internet and communications intermediaries to play a role in preventing and rectifying [technology-related] violence, harassment and bullying. The legislation recognises that *electronic communications often facilitate anonymity, which can be a barrier to accessing justice for violence against women online*. It therefore places a burden on electronic service providers to respond to requests for information about the identity of the harasser (in South Africa and Nova Scotia), to cease providing service upon the order of a court (in Nova Scotia) and even to remove offensive content when service providers become aware of its presence on their sites (New Zealand). In South Africa, an individual within a company as well as the company itself can bear criminal liability for failing to comply with a court's request to facilitate the identification of an individual accused of online harassment.[63]

Such liability has been recognised across these national contexts as an important measure. With regards to companies respecting human rights, such liability is also not beyond the scope of the UN Guiding Principles, which compels states to provide a legislative framework that upholds human rights, and positively directs companies in their related responsibilities.[64] *The*

[60]Israel passed the "Prevention of Sexual Harassment Law" in January 2014, which made the distribution of sexually explicit images or photos without the full and free consent of all parties involved a crime punishable by up to five years in prison. See: www.law360.com/articles/499212/israel-criminalizes-revenge-porn-in-new-bill

[61]Singapore passed the "Protection from Harassment" law in March 2014, which includes provisions on harassment via digital means. See: www.singaporelawwatch.sg/slw/attachments/39777/General2%20(3).PDF

[62]For current details on US legislation dealing with the specific issue of what is labelled "revenge porn", see: www.ncsl.org/research/telecommunications-and-information-technology/state-revenge-porn-legislation.aspx. For details on US states that have cyber stalking and cyber harassment laws, see www.ncsl.org/research/telecommunications-and-information-technology/cyberstalking-and-cyberharassment-laws.aspx. For details on US state laws addressing cyber bullying among young people, see: www.ncsl.org/research/education/cyberbullying.aspx

[63]Nyst, C. (2014). *Technology-related violence against women: Recent legislative trends,* p. 23. APC. www.genderit.org/sites/default/upload/flowresearch_cnyst_legtrend_ln.pdf

[64]Section 1.B.3 of the UN Guiding Principles states: "In meeting their duty to protect, States should:(a) Enforce laws that are aimed at, or have the effect of, requiring business enterprises to respect human rights, and periodically to assess the adequacy of such laws and address any gaps; (b) Ensure that other

provisions in these laws necessitate that companies explicitly recognise violence against women as unlawful behaviour, and demonstrate increased and expedited cooperation in providing relief to victim/survivors within the capacities that companies have. The provisions neither go above or beyond what internet intermediaries already have place: systems for cooperating with law enforcement, takedown procedures for abusive and harmful content, and the possibility of account termination for misconduct.

Such provisions could also *compel companies to create appropriate record keeping systems specific to VAW, and to classify and share the ways in which they have responded to reports of VAW and the actions they have taken*. As this review of policies has demonstrated, companies tend to develop formal record keeping systems and clear communication guidelines and procedures only when they are legally obligated to respond to certain data requests.

For example, *habeas data* laws in Mexico and Colombia have compelled internet intermediaries in exactly this regard; Telcel's (Mexico) policy details the exact forms that must be used, the specific department that will deal with the complaint, the timeline for action demanded of both parties, and the method of correspondence that will take place. Similarly, US-based services tend to provide the same level of detail about their procedures for compliance with the Digital Copyright Millennium Act (DCMA). Across the board, companies' legal departments maintain records of (non)cooperation with governments and law enforcement – and it is this liability that has compelled at least a few companies reviewed here (Facebook, Google, Microsoft, Twitter, WordPress) to disclose details on their cooperation with requests for user data in their "transparency reports".[65] Google has a particularly elaborate transparency portal, where it details content-takedown requests by "reason", including categories for "impersonation", "hate speech", "violence", and "bullying/harassment".[66] Google's model is a small step towards providing greater information on responses to technology-related VAW, and could be expanded upon and incorporated by other companies' reporting systems as well.

It is also pertinent to note that *the six company representatives interviewed here – from AirTel, BH Telecom, ETB, Google-Colombia, Microsoft-Colombia and YouTube – all affirmed the importance of a system of checks and balances; that the power for investigations into harassment, threats of physical safety, sexual violence, kidnapping (etc.) must lie with courts and law enforcement; and that therefore laws that direct companies in their responsibilities are necessary*. In light of the recognised merits of particular liability measures to address technology-related VAW, the question across contexts remains as to how laws and corporate policies find the right balance between the need for the retention of certain data, and the use of data in redress for acts of technology-related VAW.

---

laws and policies governing the creation and ongoing operation of business enterprises, such as corporate law, do not constrain but enable business respect for human rights; (c) Provide effective guidance to business enterprises on how to respect human rights throughout their operations; (d) Encourage, and where appropriate require, business enterprises to communicate how they address their human rights impacts." Available at: www.ohchr.org/Documents/Publications/GuidingPrinciplesBusinessHR_EN.pdf

[65]ICT companies' "transparency reports" generally provide information on the number of requests received from governments for user information or to take down content, and the percentages of requests companies have complied with.

[66]google.com/transparencyreport/removals/government

Section IV. Committing to human rights

Beyond the UN Guiding Principles on Business and Human Rights, other international initiatives on business and human rights include the UN Global Compact, the UN Women's Empowerment Principles (WEP), and the Organisation for Economic Co-operation and Development (OECD) Guidelines for Multinational Enterprises (MNEs).

- *The UN Global Compact* is the largest voluntary global initiative on corporate citizenship. To date there are more 8,000 business participants and other stakeholders involved across more than 135 countries.[67]
- *The Women's Empowerment Principles (WEP)* is a joint initiative between UN Women and the UN Global Compact. The WEP CEO statement of support "encourages business leaders to use the seven Women's Empowerment Principles as guide posts for actions that advance and empower women in the workplace, marketplace and community, and communicate progress through the use of sex-disaggregated data and other benchmarks".[68] At the time of writing, it had 780 signatories.
- *The OECD Guidelines for MNEs* are government-backed voluntary standards guiding MNEs in responsible business conduct in diverse areas, including human rights and consumer interests. The guidelines apply to MNEs incorporated within OECD member countries, including the US, the EU and Mexico.[69]

While these voluntary global initiatives and guidelines have generated interest and participation from hundreds of businesses across the globe, *only two of the 22 companies reviewed here* – some of whom are the largest international and national players in the ICT industry – *have a formal commitment to human rights: ETB (Colombia) and Microsoft (United States)*.

In an interview with the Colombia research team, a representative from ETB (Colombia) discussed the company's decision to sign on to the UN Guiding Principles. The company officially put forth its company-wide policy on human rights in 2012. Throughout the previous year, ETB held dialogues with multiple stakeholders working on business and human rights to gain insight and recommendations on the design of its human rights policy. The company also intends to implement a record keeping system on its compliance with human rights in 2015, though the budget for this was not approved at the time of writing this report. ETB has been a member of the UN Global Compact since 2005, and while it has not signed the UN Women's Empowerment Principles, the company has worked with prominent women's rights organisations within Colombia to host events, for example, on International Women's Day. The company has also implemented trainings on human rights, labour rights, and gender equality since developing its human rights policy. While positive steps are being taken, the representative suggested that *the biggest obstacle to developing these human rights-compliant methods within the company is gaining widespread support at the highest levels of management to authorise budgets towards developing such initiatives*.[70]

[67] unglobalcompact.org

[68] weprinciples.org

[69] mneguidelines.oecd.org/text

[70] Colnodo. (2014). Interview with ETB representative. Unpublished.

Microsoft joined the UN Global Compact in 2006. It has also signed up to the UN Guiding Principles and developed a company-wide policy statement on human rights. In line with its efforts, the company has created a "Technology and Human Rights Centre" tasked with improving human rights-compliant practices within the company, as well as raising public awareness, increasing dialogues between businesses, and supporting research initiatives on the impacts of ICTs on human rights.[71] Microsoft has also recently signed in support of the UN WEP though it is unclear what empowerment programmes and practices the company has yet developed.

Corporations who disregard users' concerns may only be motivated by threats to their profits, as the cases of Facebook and Twitter demonstrate. It was not until advocates created a massive public campaign and asked advertisers to pull their spots from Facebook and Twitter that these companies responded and publicly commented on the issue of gender-based hate and abuse. Within the frame of corporate social responsibility, however, those few companies that are industry leaders on human rights may be key allies in raising awareness on the issue of technology-related VAW, and can use their business relationships to encourage other companies to follow suit.

[71] microsoft.com/about/corporatecitizenship/en-us/working-responsibly/principled-business-practices/HumanRightsCenter.aspx

Section V: Summary and recommendations

The previous sections have outlined some of the key trends and tensions when addressing technology-related VAW within the current corporate policies and reporting mechanisms of internet intermediaries, particularly in response to women's experiences as documented within the research. These discussions are aimed to act as entry points that advocates can use for discussions on how to better facilitate women's access to justice through company policies in cases of technology-related VAW.

This report concludes below with (a) a summary of some of the key mechanisms in place regarding the abuse of users' rights, (b) insights for lobbying by anti-VAW advocates, and (c) areas for further research.

1. Information for individuals seeking redress

Terms of service are legal contracts between companies and their users, outlining the responsibilities of each party. ToS primarily serve to protect corporations from any legal liability and damages resulting from the use of their services and their operating procedures; yet these policies also demonstrate what a company views as (un)acceptable behaviour and a breach of terms. No matter how limited, *the ToS and their processes may serve as a space within which individuals can access certain remedies*. Individuals concerned with privacy and security should be aware of the ToS of any platform.

Most of the larger web-based social media and networking platforms (Facebook, Twitter, Google+, WordPress and other blog-hosting sites, YouTube, etc.) now have *tools to increase individual safety and security online*. These include methods by which to:

- Report inappropriate and/or abusive content (photographs, videos, comments, blog posts, pages)
- Report and/or block an abusive user from contacting you
- Report privacy violations, including fake profiles and the publishing of private or identifying information.

Generally, "Report" buttons and forms can be found:

- Located next to each function (such as the comment section, underneath photos, or message inboxes)
- In a navigation menu or sidebar
- In various "Safety", "Security", "Privacy", "Community Standards", or "Policy" centres/pages/settings. Users should keep in mind that each platform is different and often, reporting mechanisms are not centralised.

When filing a complaint or reporting content, users should *keep detailed records (e.g. photographs, screenshots, emails, recordings of conversations) of all communications with the company* – including the time, date and wording of reports, responses and decisions.

Individuals' records can then be used to hold companies accountable for their decisions on reports and complaints.

Companies may not list all of their legal obligations or reporting mechanisms and procedures online; therefore users may need to *telephone headquarters and hotlines to request all pertinent information for recourse*. Individuals may need to file official requests with a company's legal department.

For threats to physical safety, police and investigative services are the first point of entry. Court orders, police warrants, or directives from cyber crime units are typical steps taken before companies divulge identifying information on abusive users to law enforcement. These must be availed of through formal legal reporting mechanisms.

Emergency disclosure mechanisms may exist for companies to expedite cooperation with law enforcement, and law enforcement can contact companies through official channels in this regard. However, international cooperation with law enforcement depends on whether bilateral or multilateral treaties between countries exist.

The terms of service generally detail which national laws and jurisdiction the sales contract is bound by, and therefore under which jurisdiction formal complaints will be processed and handled.

Larger national and international companies tend to have specific point people to address trafficking and child exploitation, which is useful in cases of violence against girls who are under 18 years old.

Local ICT industry regulatory authorities may present an alternative forum for complaints if users feel a company is in breach of its responsibilities and obligations towards consumers.

2. Strategies for advocates

Some strategies to engage companies on the issue of technology-related VAW are:

- Organise media campaigns to raise awareness on technology-related VAW, calling on companies to:
    - Cooperate formally with anti-VAW groups and women's rights groups to input into policy formation and planning.
    - Fund research, education and prevention initiatives on issues of bullying and harassment, especially from a gendered-perspective.
    - Create legal information centres that detail the laws and liability measures that a company is governed by, including any voluntary initiatives from pertinent ministries.
    - Build upon transparency reports and formal annual reports to include specific details of how the company has addressed VAW, as well as other human rights abuses.
- Lobby industry leaders and other companies to use their business relationships to pressure ICT platforms and services to take a formal stand against VAW.

- Input into the drafting of new or amended legislation surrounding issues of technology-related VAW, including reviews of liability and systems of judicial oversight for companies on this topic.
- Support ICT platforms and services that demonstrate a commitment to anti-VAW work and human rights, which can encourage greater competition and reflexivity within the industry.
- Explore the possibility to build on companies' existing awareness of the roles that technology plays in facilitating sexual violence, exploitation and trafficking. Companies have engaged in multistakeholder dialogues, joined state ministry-initiated action plans, developed hotlines, dedicated specific departments to deal with the issue, and developed ways to expedite content takedown and cooperation with law enforcement. Such initiatives could be built upon to address certain types of technology-related VAW.

3. Areas for further research

The steps discussed within this report are by no means exhaustive. Further research is necessary to deepen the discussion on response and prevention strategies that companies can and do employ. This includes research that systematically documents *(a) women's/girls' attempts to report content and privacy violations to specific companies, (b) the responses they received, and (c) the timeline of (in)action*. Building this evidence base will highlight where where key gaps in women's access to justice lie, and provide a valuable resource for those concerned with laws and policy formation around VAW, business and human rights.

Annex 1. Ensuring compliance with the UN Guiding Principles: A checklist for addressing violence against women

Policy commitment	
1.	Does the intermediary have a publicly available statement of policy that stipulates the organisation's policy with respect to violence against women (in all of its forms)?
2.	Has the intermediary taken due diligence steps to understand the way in which it may be facilitating violence against women, in order to inform its policies and procedures?
Due diligence	
3.	Has the intermediary engaged in meaningful consultation with women, either by soliciting the input of users or by engaging women's rights groups and activists, to understand the potential adverse impacts of its services on women's rights?
4.	Is responsibility for addressing issues of violence against women assigned to the appropriate level and function within the intermediary?
5.	Do internal decision-making processes enable effective responses to issues of violence against women?
6.	Does the intermediary track how effective its responses to issues of violence against women are, either by tracking indicators or seeking feedback from affected stakeholders?
7.	Does the intermediary publicly communicate both the occurrence of, and its response to, issues of violence against women?
Remediation	
8.	Is there a grievance mechanism in place for individuals or communities who are adversely affected by violence against women?
9.	Does the intermediary consult stakeholder groups on the design and performance of the grievance mechanism?
10.	Does the mechanism meet the following effectiveness criteria?
	10a. Legitimacy – Is the mechanism viewed as trustworthy, and is it accountable to those who use it?
	10b. Accessibility – Is the mechanism easily located, used and understood?
	10c. Predictability – Is there a clear and open procedure with indicative time frames, clarity of process and means of monitoring implementation?
	10d. Equitable – Does the intermediary provide sufficient information and advice to enable individuals to engage with the mechanism on a fair and informed basis?
	10e. Transparent – Are individuals kept informed about the progress of their matter?
	10f. Rights-compatible – Do the outcomes and remedies accord with internationally recognised human rights?
	10g. Source of continuous learning – Does the intermediary draw on experiences to identify improvements for the mechanism and to prevent future grievances?