

End violence: Women's rights and safety online

GOOD QUESTIONS ON TECHNOLOGY-RELATED VIOLENCE

by Namita Malhotra

INTRODUCTION

1. What is technology-related or technology-mediated violence against women?

Violence against women has been defined by the United Nations Declaration on the Elimination of Violence against Women (DEVAW) 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.”¹ This definition includes violence in the family, in the community, and violence perpetrated or condoned by the state, wherever it occurs. Under General Recommendation 19 of the Convention on the Elimination of All Forms of Discrimination against Women (CEDAW),² violence against women is considered a form of “discrimination” which states parties to the Convention are obligated to address and eliminate.

Technology-related violence against women (VAW) falls within this definition of violence but is mediated via phone, internet, social media platforms, etc. It is acts or behaviours that cause harm or suffering, both mental and physical, and is increasingly becoming part of women's experience of violence as well as part of their online interactions. From a study conducted by the Association for Progressive Communications Women's Rights Programme (in Bosnia and Herzegovina, Colombia, Kenya, the Democratic Republic of Congo, Mexico, Pakistan and the Philippines) these were the instances of technology-related violence found:

- Taking and/or uploading and distributing intimate photos and/or videos without consent: the woman agreed that the photographs be taken for personal consumption, but did not consent to sharing the photographs; the girl/woman was unaware she was being videotaped during a sexual act, then the video was uploaded and distributed online.
- Altering photos/videos and uploading in pornography sites: a photo of the woman's face was attached to the naked body of another woman and later uploaded to pornography sites, then tagged with the woman's profession and city.

1 www.un.org/documents/ga/res/48/a48r104.htm

2 www.un.org/womenwatch/daw/cedaw/cedaw.htm

GOOD QUESTIONS ON TECHNOLOGY-RELATED VIOLENCE AGAINST WOMEN AND OTHERS

- Harassment: women receiving insulting text messages; receiving comments and messages online using sexualised insults.
- Stalking: activities monitored online.
- Blackmail/threats: a girl receiving messages asking her to have sex or her family will be harmed; a woman threatened that her intimate photos will be made public unless she goes back to having a relationship with the perpetrator.
- Accessing and/or dissemination of private data: email account hacked; accessing a woman's social network account and messaging her contact list without her knowledge; leaking private documents and information to the public.
- Creation of fake profile/identity theft: profile containing the name and picture of the woman but with derogatory descriptions such as "stripper", "Durex tester" and "professional whore".
- Hate speech: calling for women to be murdered, raped, etc.
- Child pornography: children forced to pose naked and perform sexual acts using video-chat.
- Rape/sexual violence: woman forced to have sex.³

Technology-related VAW infringes on women's right to self-determination and bodily integrity. It impacts on women's capacity to move freely, without fear of surveillance. It denies them the opportunity to craft their own identities online, and to form and engage in socially and politically meaningful interactions.

2. "Technology-related VAW is not a serious offence. Other rights issues should be addressed before taking technology-related VAW into account for legal change."

It is clear that technology-related VAW covers a range of behaviour and actions that are invasive of privacy and bodily sovereignty. Yet since these offences use technological means, often the incidents are not taken seriously. This is most often the case in countries where there is a culture of impunity and lack of accountability, and where cases of rape and sexual assault are infrequently reported and prosecuted. In

these circumstances, incidents of technology-related VAW are doubly trivialised, with factors such as class, caste, ethnicity and race playing a role.

If violence against women is taken seriously in judicial and social culture, then this necessarily includes crimes of harassment, stalking, voyeurism, etc. that are mediated through technology. *Technology-related violence exists in a continuum, and often what are seen as "merely virtual" threats soon translate into physical violence and threats to the life and safety of individuals.* A common fallacy is that prevention and redress should be concomitant with the offence: this means that if harassment or stalking takes place online then it should be addressed online or only through technological means. It would in fact be preferable to address the level of seriousness of the threat posed by the offender; for example, a protection order against someone making threats of violence and sexual assault would be more effective than blocking their phone or disabling their account when they can easily open a new one.

The perception is often that the violence that takes place online is not "real" and is therefore less harmful. Another perception is that if violence is not physical, then it is not as damaging. However, mental cruelty and psychological violence are recognised both in international law and in most national jurisdictions. The UN DEVAW recognises all kinds of violence: "physical, sexual or psychological harm or suffering". However, in certain contexts, such as where violence against women is endemic (Pakistan) or where there is already a collapse of regulatory structures and corrupt and oppressive regimes (Colombia), this can further lead to the discounting of technology-related VAW.

Incidents of technology-related VAW are also increasing because of the growing use of technology that can exacerbate existing structures of patriarchy and heteronormative⁴ oppressiveness. In most countries, what is required is an overhaul of all laws relating to sexual assault, violence and harassment. If the experience of women and others who are vulnerable because of gender or sexuality is taken into consideration, then all forms of violence, including those

³ Women's Legal and Human Rights Bureau, Inc. (2014). *Building Women's Access to Justice: Domestic legal remedies for cases of technology-related violence against women – Final research report for the APC "End Violence: Women's rights and safety online" project.* APC, upcoming.

⁴ Heteronormativity is the belief that people fall into distinct and complementary genders (man and woman) with natural roles in life. It asserts that heterosexuality is the only sexual orientation or only norm, and states that sexual and marital relations are most (or only) fitting between people of opposite sexes. Consequently, a "heteronormative" view is one that involves alignment of biological sex, sexuality, gender identity and gender roles. Source: <https://en.wikipedia.org/wiki/Heteronormativity>

GOOD QUESTIONS ON TECHNOLOGY-RELATED VIOLENCE AGAINST WOMEN AND OTHERS

mediated by or related to technology, will be listed, and thus recognised in the law.

3. Why is technology-related violence against women not taken seriously by police, courts and other administrative systems?

In countries where it is possible to file complaints for technology-related VAW either under new laws or older laws on defamation and obscenity, such complaints are often trivialised. When women report to the police, the police can be unaccommodating or dismissive. When they bring their concern to the authorities, it is hard to even get a police report filed, because of the failure of the authorities to recognise online threats and harassment as VAW or possible crimes. There is also the added social stigma of making such a complaint, disapprobation from family and community, and often disregard for the privacy of the complainant both in the media coverage and by the police. The heteropatriarchal⁵ culture that does not value the autonomy or sovereignty of women and other vulnerable people, like transgender or intersexed persons, needs to be combated through raising awareness, legal change and other tools.

Another fallacy is that technology-related VAW has an impact only on elite women. An anti-trafficking task force in the Philippines tracked down a child pornography ring in a small coastal town, where adults, including parents, were forcing children to pose before webcams. The Philippines is one of the most gender equal countries in Asia, and fifth in the world, and yet there are incidents of revenge porn and exploitative pornography that target women and children who are vulnerable because of poverty. Even in remote villages in Pakistan and Mexico there have been instances of intimate videos being leaked and other cases of technology-related VAW.

Poverty and a lack of social security make it more difficult to access systems of justice, which in turn makes it more difficult for those outside cities, with limited direct

access to technology and outside circles of privilege, to access justice for technology-related VAW. Across the global South, there is violence and exploitation of those who are vulnerable, coupled with a culture of impunity and male power, which make it necessary to have stronger legal frameworks that protect those at risk.

4. Is it only women who are “victims” or survivors of technology-related violence? What about other people who are excluded from the mainstream or are vulnerable, e.g. transgender people, minorities or ethnic groups, etc.?

A specific law for technology-related VAW is essential in most countries because women face violence and harassment on a daily basis within heteropatriarchal societies and because of the impunity of male power vis-à-vis the law. This vulnerability to structural violence and exclusion is not limited to women, but is also part of the experience of transgender and intersexed people, and often even experienced by minority and ethnic groups that are in grossly unequal relations to those in positions of power or authority (for instance, Tibetans in China, Dalits in India, etc.). For such minority and ethnic groups, there should be specific additional provisions for their protection from hate crimes and hate speech.

In relation to gender-related violence that is technologically mediated, there is a need to extend the categories of those vulnerable to include women, transgender and intersexed people. Children should also be protected, but there are already specific United Nations protocols on child pornography and trafficking and on children’s access to sexual material.

Transgender and intersexed people face transphobia, harassment and violence and this should be considered in the formulation of laws that deal with sexual assault and technologically mediated violence. Often transwomen and transmen are subject to intimidation and fear, offline and online, and are victimised and bullied. A recent instance of harassment was the editing of wiki pages to misgender public figures or celebrities⁶ who have transitioned. In several Asian countries there is or has been cultural and social acceptance of transgender people, and a recent judgment from India reflects the growing acceptance of the need for welfare schemes for transgender people.⁷

5 Heteropatriarchy ensures male right of access to women. Women’s relations – personal, professional, social, economic – are defined by the ideology that woman is for man. Heteropatriarchy is men dominating and de-skilling women in any of a number of forms, from outright attack to paternalistic care, and women devaluing (of necessity) female bonding. Heteropatriarchy normalises the dominance of one person and the subordination of another. The logic of heteropatriarchy includes the invisibility of lesbians, the construction and tolerance of dominant male violence, together with intolerance of female violence against abusers or blaming the “feminine” victim. Source: Hoagland, S. (2003). Heteropatriarchy. In Code, L. (Ed.), *Encyclopedia of Feminist Theories*. New York: Routledge.

6 Sola, K. (2014, August 22). Wikipedia: Transphobic Edits Came from Congressional Source. *Mashable*. mashable.com/2014/08/21/congressional-ip-address-linked-to-transphobic-wikipedia-edits

7 National Legal Services Authority vs. Union of India and others, 15 April 2014. supremecourtofindia.nic.in/outtoday/wc40012.pdf

GOOD QUESTIONS ON TECHNOLOGY-RELATED VIOLENCE AGAINST WOMEN AND OTHERS

Violence against women and transgender people that is mediated through technology is indicative of the limits of both sexual and technological citizenship – who can and cannot determine their own lives, desires and bodies, and who can access technology for their own needs rather than being at the mercy of technologies of the state.

LAW

5. In most countries the law for violence against women is not adequate. Shouldn't we first address laws for sexual assault, before turning to technology-related VAW?

Offences related to violence against women are mostly contained in penal laws, and often fall short of the provisions established by the UN Declaration on the Elimination of Violence Against Women or by General Recommendation 19 of CEDAW. In Bosnia and Herzegovina, for example, provisions relating to VAW can be found in the penal code under criminal offences against sexual freedom and morality. Pakistan and the Democratic Republic of Congo (DRC) have laws that look at VAW as violations against a woman's modesty and violations against good morals and public morals, respectively. In Kenya and the DRC, VAW can be found under the sexual offences acts. Under these laws, VAW is closely tied with morality, only women can be "victims", and often sexual assault is only defined in terms of penile penetration. These categorisations automatically limit the laws' applicability and fail to recognise the multiple forms of violation that exist.

Some countries, such as Colombia, Mexico and the Philippines, recognise psychological violence in their laws, and this can to some extent cover technology-

related VAW. In other jurisdictions (Bosnia and Herzegovina, India) there is a similar recognition of mental cruelty or psychological violence but only in relation to domestic violence within family and marriage, so this does not extend to cases of technology-related VAW committed by those not in such a relation to the person.

Technology-related VAW often exists in a continuum: most women face violence that extends from online to offline and is not limited to a technological device or platform. For example, harassment and stalking often lead to physical violence, or sexual assault is captured via images that are then circulated online.

Thus, what is needed is a review of legislation relating to VAW, and this must include technology-related violence because only then would it cover the range of violence that women and other vulnerable people face.

6. What are the legal remedies to deal with technology-related VAW in different countries?

APC has conducted a study of the existing legislation in seven countries, shown below in a table of international obligations, civil and criminal remedies. In some countries there are specific laws for technology-related VAW and others rely on a combination of offences in the existing penal and civil law system, even if these provisions are outdated or rely on language that emphasises the need to protect the chastity or virginity of women (see Table 1).

7. What about the right to privacy that exists in many countries? Why is this not enough?

Countries such as the Philippines, India and Myanmar have recognised the right to privacy, often in their penal laws, laws related to ICT and/or as a constitutional

Table 1.

Summary of existing laws that may address technology-related VAW

Country	CEDAW ratification	Gender equality law	VAW law	ICT-VAW law	Civil remedies
Bosnia and Herzegovina	✓				✓
Colombia	✓		✓		
Democratic Republic of Congo	✓				
Kenya	✓			✓	
Mexico	✓	✓	✓	✓	
Pakistan	✓				
Philippines	✓	✓	✓	✓	✓

* This table is taken from: Women's Legal and Human Rights Bureau, Inc. (2014). Op. cit. It is an overview and may not provide an exhaustive list of the available laws in cases of technology-related VAW. Only documents available in English were reviewed in the mapping of available laws, thus some laws might not be included in the list.

GOOD QUESTIONS ON TECHNOLOGY-RELATED VIOLENCE AGAINST WOMEN AND OTHERS

right. Further, most multinational companies offering web-based services, such as Google, Facebook and others, abide by some minimum standards for protection of privacy.

Feminists have had a longstanding problem with the notion of privacy as articulated in terms of the domestic realm or the home, because it allowed for the creation of a private sphere sanctified by culture and patriarchy within which women were often “victims” of violence or their mobility and employment outside the home were suppressed. At the same time, privacy is critical for survivors of VAW, as it allows them to access life-saving information and take steps to keep violence out of their lives.

The right to privacy is often recognised in the constitution and penal law of many countries, and so it can become a strong mechanism to buttress the rights of women in the context of technology-related VAW, especially in relation to “revenge porn” (explained in more detail later).

8. Should technology-related VAW be a criminal or civil offence? Can't we use civil remedies to address the increasing incidents of violence against women that use technology?

Technology-related VAW covers a range of behaviours and actions, and ideally both civil and criminal remedies should be available. Some legal innovations to address technology-related VAW have emerged in countries such as South Africa, after extensive consultations with local women's groups and civil society.

In *South Africa*, a possible remedy against online and offline harassment is under the Protection from Harassment Act 2010, under which victims can apply to court for a *protection order* for up to five years. Here, harassment is defined to include both online and offline harassment, whether within domestic relations or by others. Similarly, the Canadian province of *Nova Scotia* provides for a protection order in the case of cyber bullying, which includes punishment through a fine and confiscation of electronic devices. Cyber bullying is also a tort, which offers the option of recovering damages from the offender, although only through a lengthy civil trial.⁸

In certain Asian countries, however, civil and criminal laws of defamation are not accessible to the ordinary citizen and are more often used to muzzle dissent and freedom of the press (Myanmar, Thailand). Civil

and tort remedies are usually expensive litigious processes, but certain mechanisms from civil and family law such as the protection order should be used in instances of technology-related VAW. In several studies conducted by APC, it was found that the harm suffered must be addressed effectively and this can be done either by take-down of the offending material or by granting a protection order.⁹

9. In my country the system is hardly able to deal with cases of VAW (2% of rape cases lead to a conviction). What options remain for women? What should we be lobbying for?

The findings from the study carried out in seven countries by APC on technology-related VAW led to these findings:

- In most countries there is a need for specific provisions for technology-related VAW criminal offences.
- Both civil and criminal remedies are necessary.
- Law enforcement only deals with “serious” or more technical crimes.
- Gender-related crimes are not a priority for police.
- There are only related bills, rather than acts, or non-functioning cyber crime units in most countries.¹⁰

In certain countries there is a culture of impunity and male power entrenched in institutions of the judiciary and police that make it difficult to prosecute violence against women. Instances of technology-related VAW are most often dealt with through out-of-court settlements rather than lengthy or corrupt trials (Pakistan, Philippines). In the Democratic Republic of Congo, Bosnia and Herzegovina and Colombia, women have suffered from mass rapes and impunity remains a problem. In Mexico, the fight against drugs, the extreme violence around the country and the general context of insecurity have invisibilised the murders of women. With public policy and legislative reform carried out in the name of “national security”, even basic civil rights are being challenged.

One useful regulatory or legal measure would be the amendment of outdated language in colonial laws, especially penal laws, which emphasise the modesty and/or chastity of the woman. There needs to be a *shift in this language from a protectionist policy to one that recognises the autonomy of women and other vulnerable*

8 Nyst, C. (2014). *Technology-related violence against women: Recent legislative trends*. APC. www.genderit.org/sites/default/upload/flowresearch_cnyst_legtrend_in.pdf

9 Women's Legal and Human Rights Bureau, Inc. (2014). Op. cit.

10 Ibid.

GOOD QUESTIONS ON TECHNOLOGY-RELATED VIOLENCE AGAINST WOMEN AND OTHERS

groups, their sovereignty over their own bodies and lives, and the full extent of their citizenship. This also allows for granting legitimacy to the subjective experience of the woman as the essential factor in determining what is violence/assault and harassment.

10. Which countries have specific laws to deal with technology-related VAW?

Some countries have laws that specifically deal only with technology-related violence against women and other vulnerable people – the Philippines, Nova Scotia (Canada), South Africa, Kenya, India and the United States, among others.

In the US state of California, a new misdemeanour of disorderly conduct was created to deal with instances of revenge porn. New Zealand has a gender-neutral law (i.e. it covers people of all genders) that deals with all harmful digital communications with both civil and criminal remedies, and which has created new criminal offences in cases of serious harm. The Philippines amended the colonial Spanish law on sexual assault and violence in 2004, and subsequently passed the Anti-Photo and Video Voyeurism Act in 2010, which deals with voyeurism and revenge porn. India has included some provisions on voyeurism and stalking in a recent amendment to penal law. See also Table 1 above.

Bosnia and Herzegovina's penal code contains provisions relating to the unauthorised recording, photographing or filming of another person in his/her personal premises without that person's consent, or the distribution to a third party of such material without consent. Kenya has a cyber crime law under which the improper use of computer systems includes sending messages that are grossly offensive or of an indecent, obscene or menacing character; or sending messages that one knows to be false for the purpose of causing annoyance, inconvenience or needless anxiety to another person. These laws specifically list components of technology-related VAW, compared to gender equality laws or VAW laws. The provisions of the penal laws factor in the presence and the nature of ICT in defining the acts which they seek to penalise.

In other countries where specific laws or provisions for technology-related VAW do not exist in civil or criminal law, other provisions are used. For instance, in Myanmar, the criminal provision penalising obscene publications along with offences for "outraging the modesty of women" (both inherited from colonial laws) are used to prosecute revenge porn. This combination of prosecuting obscenity and harassment was also used in India prior to the amendment of the law to include some instances of technology-related VAW.

11. What steps do the police and judiciary have to take to make any law for technology-related VAW effective?

To make the law effective, what is needed is for the police and judiciary to have more knowledge on technology-related VAW – how it is committed and who can be held liable. Staff employed in companies and multinational enterprises also need to be trained on how to deal with complaints. Women have to be aware that behaviour and acts that cause suffering and harm are in fact offences.

Currently, cases of technology-related VAW are trivialised. When women report them to the police, the responses are either unaccommodating or dismissive. When complainants bring their concern to the authorities, cases tend to not reach the stage of filing a police report because of the failure of the authorities to recognise online threats and harassment as either VAW or as possible crimes under the penal code. In Mexico, for instance, the public prosecutor told two survivors that they could not file a complaint because no crime had been committed, even though it is recognised by the penal code, and despite direct threats and defamation affecting personal integrity. In Pakistan, one survivor did not want to report the threats she was receiving for fear that she might be accused of blasphemy and that the police would just say, "You deserved what happened to you."

12. What is "revenge porn"?

"Revenge porn" is a gross violation of a woman's privacy where private and sexually explicit video and photographic images are published without explicit permission and consent onto various websites for the purposes of extortion, blackmail and/or humiliation. In India and the Philippines, episodes of revenge porn have led to amendments of the law to accommodate voyeurism and other instances of technology-related VAW as criminal offences, and in the United States revenge porn is recognised as a criminal misdemeanour. A court in Germany has also ruled that a person (in this instance, a woman) can request that her ex-lover be asked to remove all photographs of her from any storage device or computer.¹¹ This

11 Oltermann, P. (2014, May 22). Revenge porn victims receive boost from German court ruling. *The Guardian*. www.theguardian.com/technology/2014/may/22/revenge-porn-victims-boost-german-court-ruling; see also Defendant v. Applicant (names withheld), Az. 3 U 1288/13 Judgment of 20 May 2014. www3.mjv.rlp.de/rechtspr/DisplayUrteil_neu.asp?rowguid=%7B120F3614-5F89-422F-92CB-AE0D6E695023%7D

GOOD QUESTIONS ON TECHNOLOGY-RELATED VIOLENCE AGAINST WOMEN AND OTHERS

does provide some protection for a person against instances of revenge porn, and in legal terms gives more weight to the “personality right” of the person in the images vis-à-vis the intellectual property right of the person taking the photograph.

However, the term “revenge porn” is misleading, because what it describes is an act of violence, and should not be conflated with pornographic content. It refers to the motivation of wanting to get back (usually at a woman) or to take revenge for rejecting a marriage proposal, spurning advances, or ending a relationship, for being seen as “loose” or amoral, being seen with someone else or someone outside of the caste or religious community, etc. – outside the male’s control. In many ways these reasons are similar to those for which women are targeted for acid attacks in countries such as India and Pakistan.

13. Stricter laws for technology-related VAW would necessarily limit freedom of expression – true or false?

Stricter laws for technology-related VAW can offer criminal and civil remedies (most of them are amendments to criminal law) to women and other vulnerable people who face harassment, bullying, stalking and other technologically mediated violence that can often extend to physical harm. This would cover instances of wilfully leaking intimate images and conducting “sting operations” that violate the privacy of the person. The ways in which laws are drafted and the duty of the courts are meant to maintain the balance between the right to privacy of the individual as recognised in international law, constitutional law and penal laws, and freedom of expression. The only defence against charges of defamation and voyeurism or wilful exposure of private/intimate material is that the public good will be served by such a disclosure. This can clearly not be established for ordinary people or even in cases of private videos of celebrities or politicians.

Most cases of technology-related VAW are malicious attacks on the sexual and technological citizenship of women and other vulnerable people. While technology is heralded as bringing greater freedom of expression and greater efficiency, it also increases the vulnerability of those who do not have access to privileges of gender and class, such as women, minority groups, transgender people, poor people and others. Technology-related VAW impedes women’s freedom of expression by creating a violent, misogynistic culture online.

COMPANY POLICY

14. What kind of technology-related violence against women takes place via social media platforms?

A broad definition of technology-related VAW has been provided earlier, along with a list of examples of what should be covered. In relation to social media platforms such as Facebook, Google+, Twitter, Orkut and others, a recent APC study found the following specific instances of harassment, bullying, threats and other kinds of violence, involving both psychological and sometimes physical harm:

- 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/or commit blackmail.
- Pages, comments, posts, etc. targeting women with gender-based hate (misogynistic slurs, death threats, threats of sexual violence, etc.).
- Publishing personal identifying information about these women including names, addresses, phone numbers and email addresses without their consent.¹²

15. What kind of technology-related violence against women takes place via telephony services?

Mobile phones were most often used as a tool to inflict psychological and emotional violence on women and girls when physical contact was not possible, as per the study conducted by APC.¹³ In a few cases, it was unknown aggressors or strangers harassing or intimidating through calls or SMS, but in the majority of cases involving mobile phones, the harassment and intimidation was within the context of ongoing physical abuse from a known aggressor. The extended violence fell into the categories of domestic violence, intimate-partner abuse, homophobic violence, kidnapping, rape and sexual assault. State services and law enforcement are primarily responsible for enabling women’s access to justice in addressing such violence, but companies can also help provide avenues for redress.

¹² Athar, R. (2014). *Building Women’s Access to Justice: Improving corporate policies to end technology-related violence against women – Final research report for the APC “End violence: Women’s rights and safety online” project*. APC; upcoming.

¹³ Ibid.

GOOD QUESTIONS ON TECHNOLOGY-RELATED VIOLENCE AGAINST WOMEN AND OTHERS

16. What are the challenges or problems of making a complaint to a company? What are the terms of service and what protection can they give?

Most companies that provide services such as social media platforms or websites require the user to agree to their terms of service (TOS). The TOS contain clauses that prohibit the user from using the company's services for illegal purposes, and this is sometimes extended to fraudulent, abusive or indecent purposes. Even the term "illegal purposes" can be extended as per the law of the land to acts and behaviour that violate the privacy of the individual, or to the distribution of "pornographic" material, thus covering some instances of technology-related VAW. However, it is preferable that the TOS make explicit references to what is not acceptable.

In most companies, the TOS refer to illegal uses that impact the company directly, such as violation of copyright, financial fraud, extortion and child pornography, but do not specifically mention any human rights abuses, especially those based on gender, sexuality or related issues. The liability of the company via its TOS is often only a reflection of its legal obligations in its country of residence. There is common reluctance to engage directly with human rights issues.

17. What is a privacy policy and does it give protection against technology-related violence against women? Does it unfairly protect the rights of aggressors?

A company enters into a privacy policy with users which requires it to protect their data unless ordered to divulge it by a court order. Despite the bureaucracy, and the length of time this adds to processing complaints, requiring a court order before companies disclose the personal data of users is good law. It provides a system of checks and balances that limits abuse of privacy rights by governments and other state authorities, as well as by companies and individuals.

A privacy policy also ensures that this protection is extended to women, transgender people and other users who might be vulnerable. Instances of stalking by government officials (India) make this important.¹⁴ The right to privacy in the digital age is of growing importance and a balance should be maintained in law and policy between the right to privacy and the rights

14 Datta, S. (2014, May 26). Why the courts should take up 'Snoopgate' even though the woman doesn't want it probed. *Scroll*. www.scroll.in/article/665094/Why-the-courts-should-take-up-'Snoopgate'-even-though-the-woman-doesn't-want-it-probed

of women and transgender people against violence that is mediated through technology.

18. Is the complaint process of a company easily accessible and transparent to the average user?

Not many people know how to make a complaint to a multinational company. Moreover, the records of how such a process works are not easily available to determine its effectiveness, as was found during the APC study.¹⁵

Most companies do have the mechanisms in place that should technically respond to such violations (see questions 14 and 15). But there is little public information on how these mechanisms work or how effective they are – even basic information like how many complaints were received, statistics on how they were dealt with, or the kind of training on sexuality, gender, human rights and law that the staff receives. It is because of this corporate stonewalling that survivors of technology-related violence have to access remedies through the courts, even if these are slower or less effective. Also, companies often take ad hoc action without reference to their own complaint procedures and thus end up hampering the speech of the survivors of technology-related violence, or women and others who are vulnerable. Facebook's policy on breastfeeding pictures is one such example, where their mechanisms of censorship and ad hoc removal are more harmful to women than beneficial.

In addition to a lack of transparency on internal decision-making processes, no social media/networking company surveyed has a public commitment to human rights, nor demonstrates a clear understanding of violence against women, though some steps have been taken.

19. Are the staff able to respond effectively to complaints of technology-related violence against women?

The staff or personnel employed in companies need to be trained about how technology is used for violence against women in such instances and how to effectively stop or block the aggressors. Training or capacity building should include which relevant international guidelines or national laws have to be followed in relation to the company's commitment to uphold the human rights of women, vulnerable or minority groups, as well as national laws on defamation, voyeurism or other civil and criminal offences connected to technology-related violence against women. There is little understanding of how technology can be used

15 Athar, R. (2014). Op. cit.

GOOD QUESTIONS ON TECHNOLOGY-RELATED VIOLENCE AGAINST WOMEN AND OTHERS

for violence against women; for instance, a user can switch to a new account to continue abusive behaviour. In such instances the company has to find effective ways of blocking the aggressor.

Obviously, companies would be the most effective providers of remedies such as take-down of material that violates a person's privacy, or effectively blocking users who are harassing others even if they switch accounts. The presumption of most corporate policies, however, is that the only demand is identifying harassing users, and this obscures the possibility of coming up with more holistic solutions to technology-related violence against women and others who are vulnerable.

20. How accessible are the complaint mechanisms to those not living in the global North, where the headquarters of these companies are located or national law and policing are more responsive?

Multinational enterprises should detail the jurisdiction of the parent company and the subsidiaries, so users know which grievance mechanism should be used. The problem with these grievance mechanisms is often the lack of transparency in how they function. Take Back the Tech! has rated Facebook, Twitter and YouTube and graded their relative commitment to address technology-related VAW.¹⁶

In most countries not located in the global North, it is difficult to access the grievance or complaint mechanisms set up by a multinational company. Even if there are ways to "flag" content as offensive, abusive or a violation of your privacy, these complaints take a long time to be addressed and sometimes are wrongly understood. There is obviously an English language bias in reporting mechanisms, even on social media platforms that do support other languages. Efforts by such companies to include marginal or minority group concerns in their policy are confined to locations in the global North. For instance, Facebook has launched the Network of Support, comprising five US-based LGBT advocacy organisations, and in July 2013, in collaboration with the US National Network to End Domestic Violence, it released "Safety and Privacy on Facebook: A Guide for Survivors of Abuse".¹⁷ However, this engagement is limited to groups in North America and the European Union.

16 Association for Progressive Communications. (2014). *Take Back the Tech's Report Card on Social Media and Violence Against Women*. <https://www.takebackthetech.net/sites/default/files/2014-reportcard-en.pdf>

17 <https://www.facebook.com/notes/facebook-safety/safety-and-privacy-on-facebook-a-guide-for-survivors-of-abuse/601205259900260>

21. Can't companies ban or disrupt the service of the person who is misusing their services for purposes of harassment, bullying, etc.?

Technically, in most instances they can. For purposes of data retention laws or for billing, most companies have information to substantiate claims of abuse (for instance, the frequency of calls or contact made by the aggressor or the person misusing the services). Most companies, however, do not enact the disruption of services policy in relation to abusive behaviour or acts such as stalking, harassment, threats, etc. Suspending services is confined to instances when companies are owed monies. If the law of the land does not take abusive or coercive messages sent via phone or SMS seriously as threats, then in such cases (Mexico, Bosnia and Herzegovina) it is unlikely that companies would take any helpful action on behalf of the woman or other vulnerable person being targeted.

22. Aside from TOS and privacy policies, what other legal or other obligations are there to ensure that companies take action in case of a complaint?

A multinational company has to abide by the national law. Since the TOS usually prohibit illegal use of the company's service or platform, this would ensure that those acts covered under the existing national law as offences against women would be grounds for a complaint.

Other than TOS and privacy policies (which abide by laws of national jurisdiction), some international guidelines would be relevant to business operations. The United Nations Guiding Principles on Business and Human Rights (or the "Protect, Respect and Remedy" Framework of the UN)¹⁸ would be applicable to all these enterprises. The guidelines require that human rights be respected throughout the operations of businesses, and establish that it is the duty of the state or government to ensure this. Section 12 of these guiding principles establishes the responsibility of business enterprises to respect human rights, and in the commentary there is specific mention of the human rights of individuals who belong to certain vulnerable groups, i.e. the rights of indigenous peoples; women; national or ethnic, religious and linguistic minorities; children; persons with disabilities; and migrant workers and their families.

Principles of women's sovereignty over their own bodies and their rights against violence, both online and offline, as established in CEDAW and DEVAW, the

18 https://www.unglobalcompact.org/issues/human_rights/The_UN_SRSRG_and_the_UN_Global_Compact.html

GOOD QUESTIONS ON TECHNOLOGY-RELATED VIOLENCE AGAINST WOMEN AND OTHERS

principles outlined in the Optional Protocol on Child Pornography, and the rights of vulnerable and marginal groups established in civil, political and human rights documents should also be part of the commitment of most business operations, although they are technically applicable only to states that have ratified these documents.

23. Which services or platforms provide an effective complaint mechanism for technology-related VAW? What is their response when asked about their commitment to human rights and their response to violence against women or others using their service or platform?

APC's study of corporate policies¹⁹ covered the following companies: platforms such as Facebook, Twitter, Google+, YouTube, Instagram, WordPress; pornography websites such as Xvideos and YouPorn; internet portals such as Google-Colombia and Yahoo-Philippines; and telephone, mobile and internet service providers such as Telecom in Bosnia and Herzegovina, Claro ETB in Colombia, Airtel in the DRC, and national telecom services in Kenya, Pakistan, Mexico and the Philippines, among others.

The companies surveyed had *no formal public records of how their customer service departments operate*. The study looked at 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.

Moreover, even if there is a clear definition of unacceptable use in the TOS, there is *no clear, easy-to-access and transparent procedure to deal with complaints* of violations by users vis-à-vis other users on the website or platform. Such complaints of illegal or abusive behaviour need to be dealt with in a formal and timely manner beyond a general "customer service" department.

Most such companies shift the burden of dealing with technology-related VAW to the state or national government where their operations are located, or to the individuals facing harassment. Their responses are that:

- Law enforcement is responsible for addressing VAW.
- A court order is essential to protect privacy rights.
- Women and girls should take steps to keep themselves safe.

While most women's groups and feminists agree that companies must abide by privacy laws and laws for freedom of expression at an international and national level, the corporate attitude displayed to abuses of women's rights and human rights is troubling.

RECOMMENDATIONS

Recommendations for law-making institutions²⁰

- The law should recognise VAW as a human rights violation and provide a comprehensive definition of VAW to include psychological violence occurring in public and private life.
- The text of the law must change from emphasis on a woman's chastity to recognition of her autonomy over her own body and life in accordance with the universal right to self-determination. This basic change in terminology should be reflected in all laws related to violence against women.
- Changes in law for technology-related VAW should extend to others who are vulnerable because of gender – such as transgender and intersexed individuals who face harassment and violence on a daily basis.
- With regard to constitutional and criminal provisions for protecting the right to privacy, national constitutions should recognise the right to privacy of all individuals, vis-à-vis the state, corporate actors and other people. In specific criminal provisions related to voyeurism, stalking, etc., there should be recognition of the person's privacy in terms of spatial, bodily and data privacy.
- Laws for technology-related VAW should include both civil and criminal options. Laws should provide swift redress for harm and suffering via court orders for take-down of material and protection orders against harassers.
- VAW is due to a culture of male impunity, heteropatriarchy and structural exclusion of women and marginal groups from systems such as the judiciary, police, etc. There is a continuum between technology-related VAW and "offline" VAW as they both stem from the same root causes. Remedies for technology-related violence do not have to be limited to the online or virtual realm.
- Laws should balance the rights to privacy, the right against violence and harassment, and the right to freedom of expression. This is a difficult

19 Athar, R. (2014). Op. cit.

20 Women's Legal and Human Rights Bureau, Inc. (2014). Op. cit.

GOOD QUESTIONS ON TECHNOLOGY-RELATED VIOLENCE AGAINST WOMEN AND OTHERS

balance to achieve, but it must be maintained in constitutional, civil and criminal law and by the courts adjudicating over each complaint filed.

- To make the law effective, states must allocate adequate and sufficient budgets and resources to address VAW. Focus should be placed on ensuring that the police and judiciary involved in dealing with technology-related VAW are trained to effectively address the needs of women victims of violence.
- A protective, preventive and proactive approach to tech-related VAW incorporates the creation of an enabling environment for women's access to and enjoyment of ICT in terms of quality infrastructure, training in highly technical skills, and meaningful participation in internet governance for women.

Recommendations for companies²¹

- Companies, especially multinational companies, that provide internet/telephony services and social and pornography sharing platforms must abide by the United Nations Guiding Principles on Business and Human Rights (or the "Protect, Respect and Remedy" Framework of the UN), which require that all human rights be respected throughout the operations of businesses. Companies should make a formal and authentic commitment to upholding human rights and taking action to prevent and address violence against women and transgender people, even though it is the duty of the state to ensure that the guidelines are followed.
- The privacy policy of the company should provide adequate protection to those who are vulnerable to forms of violence and harassment via the company's services. This privacy policy should protect against technology-related violence, and not be a veil behind which acts of harassment and violence are protected.

- Companies should invest in capacity building of personnel, particularly in customer service departments, and also have separate procedures for dealing with complaints of technology-related violence against women and others who are vulnerable. Most of those employed in these departments are not aware of how technology can be used for violence and harassment, nor are they aware of the duties and obligations of companies to protect their users against such violence under national law, international guidelines and their own terms of service. In particular, they need to improve their ability to fully serve people who do not speak English and/or live outside of North America and Europe.
- Agreements between the user and the company, such as terms of service and privacy policies, should make explicit references to technology-related VAW (not only a general prohibition against illegal use) and they should provide a transparent and easily accessible process for filing complaints in which the privacy of the complainant is protected. Companies should cooperate formally with anti-VAW groups and women's rights groups, including groups outside of North America and Europe, for input into this policy formation and planning.
- Building upon transparency reports and formal annual reports, companies should include specific details of how they have addressed VAW, along with other human rights abuses. In particular, they should publish information on the number of reports received, responded to and acted upon, including information about complaints processes more generally, what standards are applied, and how complaints are dealt with throughout their lifecycle.
- Companies should fund research, education and prevention initiatives on the issue of bullying and harassment, especially from a gendered perspective, to address violence against women.

21 Athar, R. (2014). Op. cit.



Ministry of Foreign Affairs