## **APC** EXECUTIVE SUMMARY

# VOICES FROM DIGITAL SPACES: TECHNOLOGY RELATED VIOLENCE AGAINST WOMEN

## PART I: SETTING THE SCENE

Information and communication technologies (ICTs) are a range of technologies people use to collect, share and distribute information, and communicate. Rapid expansion of these technologies has changed the way people relate to each other and to the world. Due to ICTs, the possibility of communicating and sharing information has increased and quickened.

ICTs can be used in different ways, including to increase or to limit freedoms and rights. This can be seen in relation to violence against women (VAW) - the physical, mental or sexual harm that women experience because they are women or which affects them disproportionately. More and more women experience violence through the use of internet and mobile phones. On the other hand ICTs can be used to increase women's access to information and services necessary to protect and further their rights.

However few women's rights activists address the complex relationship between VAW and ICTs in their work. In most countries there is also little legal and political framing of this issue.

This paper is targeted at organisations and policy makers working on VAW and communication rights advocates. It explores the links between ICTs and VAW and illustrates that technology related violence impacts women as seriously as other forms of violence. It also aims to assist these audiences to incorporate this perspective into their work and stimulate action-oriented policy dialogues to address this new form of VAW.

This paper draws on the experiences and findings of the Association for Progressive Communications (APC) MDG3: Take Back the Tech! project. MDG3: Take Back the Tech! worked with women's rights organisations in twelve countries in Asia, Africa and Latin America between 2009 and 2011. The project supported these organisations to research and respond to technology related VAW and strengthened their capacity to use ICT tools in their responses to violence. The paper also builds on other APC Women's Networking Support Programme (WNSP) work in the area of VAW, women's rights, sexual rights and ICTs.



We do not aim to provide a comprehensive mapping of technology related violence or delve into all relevant debates on this area. Rather this paper explores the emerging trends and patterns of technology related violence that women are experiencing across the world and outlines ways we can respond to this.

Gender and ICT context

Globally, women experience gender-based economic, political, social and cultural inequality, including in access to rights such as education, health and safety. VAW is also prevalent in different forms worldwide. The ways in which women experience inequality and violence depend on their race, class, sexual orientation, nationality and geographic location.

Globally, women have less access to and control of ICTs and use them differently than men. In developing countries, fewer women than men use the internet. In low and middle income countries, women are 21% less likely than men to own a mobile phone. This inequality is linked to broader gender inequality that exists in these societies.

Many factors contribute to gender based differences in ICT access, use and control, including access to education, connection costs, lack of physical infrastructure, poverty, time availability and cultural attitudes. For the information society to be more accessible to women, women must be able to connect to ICTs wherever they are. Also, available content and online spaces must respond to women's needs and interests. Finally, women and their organisations must have the capacity to harness and use ICTs.

### How do ICTs connect to VAW?

Technology related violence is a form of VAW that manifests in the context of these new technologies. ICTs can be used to perpetrate violence in a variety of ways.

Perpetrators of violence use mobile phones and the internet to stalk, harass and monitor women's movements

and activities. Specifically, perpetrators use mobile phone tracking services, obtain control of passwords and monitor text messages and incoming calls. Perpetrators also use ICTs to collect and distribute intimate and sexual photos and recordings of women without their authorisation.

The most frequent forms of technology related VAW are:

- Online harassment and cyberstalking, which constitutes one of the most visible forms of VAW.
- Intimate partner violence, where technology is used in acts of violence and abuse in intimate or spousal relationships.
- Rape and sexual assault, where technology is used to track the movement and activities of women to provide location information. Also, when violence continues through digital recording and distribution of the violation. In other instances, fake internet postings or adverts have been used to attract women into situations where they are sexually assaulted.
- Culturally justified VAW, when technology plays a role in creating a culture of VAW or perpetuates the use of culture or religion to justify, ignore or accept acts of VAW.
- Violence targeting communities, where communities face targeted online attacks and harassment because of their gender or sexual identity and/or political stance.

ICTs allow perpetrators to commit violence anonymously and at a distance from the women they are targeting, making it harder to identify perpetrators and charge and prosecute them. Phone tracking services and web sharing platforms also allow surveillance of women's activities and replication and distribution of intimate photos with little cost to and effort by the abuser.

Due to the "record everything, forget nothing" memory of the internet and the possibility of endless replication of information, women experience the consequences of harassing texts and images targeted at them without the

SMA Development Fund Women & mobile: A global opportunity (GMSA, 2010) www.mwomen.org/Research/ women-mobile-a-global-opportunity\_1

ability to stop them.

In many cases of violence, the perpetrators are numerous. For example, in the unauthorised distribution of private images, there is often a sole principal perpetrator – the person who posts images. Yet viewers of these images and people who re-circulate them are additional perpetrators. Similarly, online harassment often involves multiple abusers who post sexually harassing comments and threats.

These acts of violence violate a range of women's rights, including a woman's right to privacy and protection of personal and sensitive information.

Feminist researchers argue that within the context of ICTs, the body transcends the physical. Consequently, the distribution of intimate and abusive representations of bodies violates women's right to bodily integrity and autonomy.

Furthermore technology related violence affects women's freedom to express themselves, move freely online and enjoy online communities, violating their autonomy, freedom of expression and access to information.

The harm that women experience through this violence is mainly psychological and emotional, including fear, anger, stress and depression. Moreover, online abuse can escalate into offline physical abuse if not checked. Technology related violence has, in some cases, led to suicide, particularly amongst young people. Women who experience this abuse are also likely to withdraw from online and offline social networks and active participation in political, social and economic life.

## How ICT policy and legal frameworks respond to VAW

ICT policies and laws do exist, including in some of the Take Back the Tech! project countries. For the most part though, they are gender blind and do not account for technology related VAW. Additionally, in legislation

protecting and fulfilling women's rights, ICTs are rarely mentioned.

The MDG3: Take Back the Tech! project documented the struggle that victims/survivors of technology related violence experience in seeking justice and claiming their rights. Legal and regulatory mechanisms and law enforcement bodies are often uncertain of what laws to apply to these cases. They consult anti-VAW laws, cybercrime bills and laws on privacy rights.

# PART II: CASE STUDY – SEXUAL VIOLENCE AND UNAUTHORISED DISTRIBUTION OF INTIMATE IMAGES OF WOMEN

## Naming and unpacking settings and manifestations

Although statistics are not available on the extent to which intimate photos and video recordings of persons are distributed without their consent, media reports, advocates and organisations working on VAW indicate that women and sexual minorities are frequent targets of these offences.

Images and recordings distributed in this form of violence are taken with or without the consent of the women targeted. In some cases, photos and recordings are taken through voyeuristic means such as hidden cameras. In other cases, women send intimate images of themselves to their sexual partners or agree to recordings being made of a sexual act with their partner. Their partners then use these images and recordings in abusive ways while they are still in the relationship or after the relationship has ended.

Abusers can also manipulate photographs of women into pornographic images and distribute them with personal information such as a phone number or address.

Instances of rape and sexual assault have also been recorded and distributed through the internet and mobile

phones by bystanders or participants in violence. For example, in 2010 in Canada, a girl was drugged and sexually assaulted by a group of men at a party. Onlookers recorded the incident and distributed it widely on the internet.

Perpetrators record these images for different reasons. In some instances, distribution threats are used to blackmail women or force them to stay in abusive relationships. Images and recordings are also distributed to embarrass and defame women who are public figures. In other cases, abusers circulate these images and recordings as a "hobby", to gain status amongst their peers or simply because they can.

Public circulation of images and recordings leads to the multiple victimisation of victims/survivors. Every time another person views or posts blaming or harassing comments on an intimate photo or recording of a woman, she is re-victimised.

#### Access to justice

Child pornography laws, privacy protection laws and anti-VAW laws, present possibilities and also limitations in providing redress for victims/survivors of unauthorised distribution of images and recordings.

### Child pornography laws

Child pornography laws criminalise the creation, display and distribution of sexual images of children. Children are defined as persons under the age of 18 or 16, depending on the country.

For this type of crime, child pornography laws provide for more severe criminal penalties than, for example, privacy laws. Currently, there is a strong will among states to investigate and prosecute child pornography crimes nationally and transnationally. This allows for the necessary international cooperation, enabling police to respond to crimes that cross national borders. However child pornography laws do not differentiate between the unauthorised or authorised recording and distribution of these images. Hence girls can be criminalised for sharing images of themselves with their romantic partners. The laws need to recognise the right of youth to self-determination and bodily integrity and distinguish between consensual and non-consensual acts. While the extent to which youth do consent to these acts on the basis of informed decision-making is an issue, the emphasis needs to be on prevention rather than criminalisation. For example, education programmes for youth can help them negotiate online spaces and sexual interactions safely.

Child pornography laws also do not recognise the gender based nature of these abuses. This is necessary for a holistic, adequate response to the needs of women victims/survivors of this violence.

### Privacy protection laws

Privacy laws protect the right to respect for private life and regulate the collection, storage and usage of information. Many states though have inadequate legislation to protect the right to privacy, effectively handing over this duty to individuals and the market.

Furthermore, privacy is often equated with state or corporate intrusion into people's lives, rather than breaches by individuals, including partners, parents or siblings.

Moreover, privacy debates are dominated by the perspectives of middle class men. Hence women's privacy concerns and technology related VAW which is defined by women's social position and which often involves privacy breaches committed by individuals, including their partners, parents or siblings, gets little attention.

Additionally, public and policy discourse on privacy is often framed by the same cultural and moral perspectives used to control women's bodies. So in many contexts, cases of unauthorised distribution of intimate images of women are seen as a corruption of social, community and family

norms rather than as violations of women's right to bodily integrity and autonomy. Consequently, the morality of the victim/survivor herself is often questioned, and the violation is seen as a shame on her.

Another layer to this discussion is how to balance an individual's right to privacy with the public's right to information, particularly in relation to public figures. For example, in Malaysia, a sex video involving a woman politician was released publicly. Calls for stronger privacy protection following this incident were watered down by debates on morality and the public's expectations of public figures.

In the Philippines, the Anti-Photo and Video Voyeurism Act of 2009 is an innovative law that penalises taking, copying and distributing photos or videos of sexual acts or of a person's private areas without the consent of the person/s involved. It provides for harsher penalties than other privacy laws and includes the possibility of imprisonment.

However, this law does not recognise that these acts can be a form of VAW and does not specify what consent means. If the implementation of this legislation places the onus on victims/survivors to prove consent, it can discourage women from reporting crimes and from seeking prosecution, as frequently happens with sexual assault legislation.

#### Anti-VAW laws

Three types of anti-VAW laws can be applied to cases of unauthorised distribution of intimate images of women: pornography laws, laws against sexual offences and sexual harassment legislation.

All three types of laws recognise these crimes against women as a form of VAW. Hence they can ensure a gender sensitive approach to investigation and prosecution of these crimes. Still, proving psychological and emotional harm and hence that an act of violence has been committed is as difficult within the framework of these laws as within the framework of, for instance,

privacy laws.

These laws need to be expanded to include definitions of violence on the basis of emotional and psychological harm to take full account of the violations that women experience online and the impact of technology related violence. They also need to reflect the blurry boundaries between online and offline violence, especially given that one form of violence can escalate into the other or be linked. For example, when sexual assault is recorded and distributed this leads to the further victimisation of women.

## Balancing freedom and "protection" in dealing with VAW

While new and innovative measures need to be developed to deal with VAW, we need to be aware of the form these solutions take. For instance, measures that take a protectionist approach to women's online safety can increase censorship by state or non-state actors and, in turn, limit women's freedoms. For example, recent policies to counter child pornography have led to search engines filtering sexually related content and lesbian, gay, bisexual and transgendered (LGBT) related terms in Arabic regions. This can restrict women's and sexual minorities' right to expression and access to information.

## PART III: CONCLUSIONS AND RECOMMENDATIONS

## Recommendations for policy-makers, ICT intermediaries, media, ICT users and organisations working on VAW

Responding effectively to technology related VAW requires action by everyone who shapes ICTs and everyone who is responsible for addressing VAW. This includes ICT users, internet service providers, the state, organisations working on VAW and the media. Action also needs to happen on different levels: to tackle the root causes of VAW and transform unequal power relations; to limit the

consequences of VAW for victims/survivors by ensuring immediate response and support; and through long term care and support for victims/survivors.

The need to engage internet intermediaries, who develop and operate internet and mobile phone platforms, has become increasingly apparent. These intermediaries are powerful players in ICT policy and shape debates and regulatory measures. However they often dismiss their critical role and responsibility in protecting their users from VAW.

#### Laws and policies

States need to create, implement and monitor laws and policies that respond to technology related VAW. Anti-VAW laws need to be expanded to account for the nature of technology related violence. Laws that deal with ICT crimes need to account for gender differences and inequalities.

Developing these laws requires a holistic perspective that assesses and balances all women's rights so that none of them are adversely affected, through for example censorship measures. Different stakeholders also need to be involved and women's participation ensured. Multistakeholder spaces such as the transnational Internet Governance Forum are good platforms for dialogues.

## Advocacy to ensure women's participation

Civil society organisations need to advocate for policymakers to take into account technology related VAW and for women to participate in policy-making spaces.

Gender report cards on the ICT sector that monitor and assess women's inclusion in forums and bodies in this sector can be useful to challenging women's under-representation. The MDG3: Take Back the Tech! project supported local partners from women's rights organisations to participate in key regional and international ICT policy making spaces. The project also

supported national dialogues with ICT and government policy-makers and women's rights organisations in the twelve countries to develop strategy plans on technology related VAW.

#### **Evidence building**

Systematic reporting and monitoring of technology related VAW is needed to support advocacy and feed into evidence based policy making. These studies should include the perspectives and participation of women from different backgrounds, races, classes, sexualities and nationalities.

APC, in collaboration with the MDG3: Take Back the Tech! campaign partners, has set up an online mapping platform<sup>2</sup> for women to share stories, news and experiences of technology related VAW. The platform records and categorises the violence reported.

## Making online spaces safer: Internet intermediaries' policies and strategies

Internet and mobile phone service providers need to ensure that women using their services understand what behaviour risks their safety and how to prevent and stop violence.

Anti-VAW experts should be included in standards setting processes. Services should also include effective complaint mechanisms to report abuses and gain assistance in stopping abuse.

ICT intermediaries can also ensure user safety from violence through the design of safer ICT services. For example profiles for social networking sites can be set as "private" by default to restrict access by strangers to view, search and comment on a user's profile.

Initiatives such as the EU Safer Social Networking Principles, the outcome of multi- stakeholder processes, can guide intermediaries on best practices for safety.

<sup>2.</sup> www.apc.org/ushahidi/

## Media literacy and empowering women users

Preventing VAW requires working with ICT users and potential victims to change attitudes and behaviour. Media literacy initiatives engage users to be more aware of the implications of their acts. For example peer education initiatives in the USA educate youth on the legal and social consequences of sharing sexual information. The Global Take Back the Tech! Campaign calls on all ICT users to take control of technology to end VAW, including through daily actions such as the "I don't forward violence" pledge.

Other initiatives work with women and girls to increase their control of technology and empower them to use ICTs effectively and securely. For example, APC builds the capacity of women human rights defenders through training on online secure communication and supports them to network via the internet and exchange experiences.

#### Mass media

People working in online and print media have a responsibility to not distribute insensitive information on victims/survivors of technology related VAW. In South Africa, after a recording of an alleged gang rape was circulated via ICTs, some newspapers gave detailed accounts of what was contained in the recording and published images of the victim/survivor's house. Information such as this violates the victim/survivor's rights and can lead to further victimisation.

The media can play a positive role in unpacking and naming this type of violence.

## Support for victims/survivors of violence

There is also a need to assist organisations working on VAW to better support victims/survivors of technology related VAW. Front line organisations need capacity building and practical tools on safe online communication and monitoring, reporting and responding to incidents of technology related VAW.

ICTs can also facilitate care and support for victims/survivors through social networking and online communities. These allow for sharing experiences and advocacy for non-violent relationships.

Furthermore, ICTs can be used in civil society solidarity campaigns to support victims/survivors of violence. For example, in Malaysia after intimate pictures of a female politician were leaked on the internet, a solidarity campaign used Facebook to mobilise support for her. This campaign played a role in preventing her from resigning her position after the incident.

#### Conclusion

This paper demonstrates that cases involving technology related VAW cause serious harm to women and are increasing. Victims/survivors of technology related VAW are moreover at risk of further victimisation by multiple perpetrators. The trends, gaps and strategies we have presented in this study are key starting points for organisations and institutions working on ICT policy and/ or women rights to stop this violence. What is most critical now is to promote strategies and policies that empower women and allow them control of their situations as opposed to adopting protectionist approaches. This needs to be at the heart of all work to end VAW.

APC WNSP would like to thank the MDG3 Fund for their support of this research.



Ministry of Foreign Affairs

Editor

Maia Marie

**Authors** 

Katerina Fialova and Flavia Fascendini

Project coordinator

Jan Moolman

Regional project coordinators

Dafne Plou Jennifer Radloff Lalaine Viado

Country project coordinators

**Africa** 

Françoise Mukuku - Si Jeunesse Savait, Democratic Republic of Congo

Goretti Amuriat - Women of Uganda Network (WOUGNET), Uganda

Lebohang Marishane, Lerato Legoabe and Sally-Jean Shackleton - Women'sNet, South Africa

Sylvie Niombo - Association AZUR Développement, Republic of Congo

Asia

Chim Manavy - Open Institute, Cambodia

Lenlen Mesina - Foundation for Media Alternatives, Philippines

Maria Abdullah - Persatuan Kesedaran Komuniti, Selangor (PKKS), Malaysia

Shahzad Ahmed and Nighat Dad - Bytes for All, Pakistan

Latin America

Beatriz Alarcón and Olga Paz - Colnodo, Colombia

Beatriz Cavazos Siller - Modemmujer / Olinca Marino and Erika Smith - LaNeta, Mexico

Carola Caride - Taller Permanente de la Mujer, Argentina

Vera Viera - Rede Mulher, Brazil

We also thank Jehan Ara for her contributions in Pakistan.

Reviewers

Aisha Shaheed Chat Garcia Ramilo Edna Aquino Erika Smith Jan Moolman Jelen Paclarin Rochelle Terman Susan Tolmay



#### ASSOCIATION FOR PROGRESSIVE COMMUNICATION

Internet and ICTs for social justice and development

APC is an international network of civil society organisations founded in 1990 dedicated to empowering and supporting people working for peace, human rights, development and protection of the environment, through the strategic use of information and communication technology (ICTs).

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

www.apc.org info@apc.org

VOICES FROM DIGITAL SPACES: TECHNOLOGY RELATED VIOLENCE AGAINST WOMEN

PUBLISHED BY APC WNSP

2011

APC-201111-WNSP-I-EN-PDF-126 ISBN: 978-92-95096-35-6

Creative Commons Licence: Attribution-NonCommercial ShareAlike 3.0 licence

