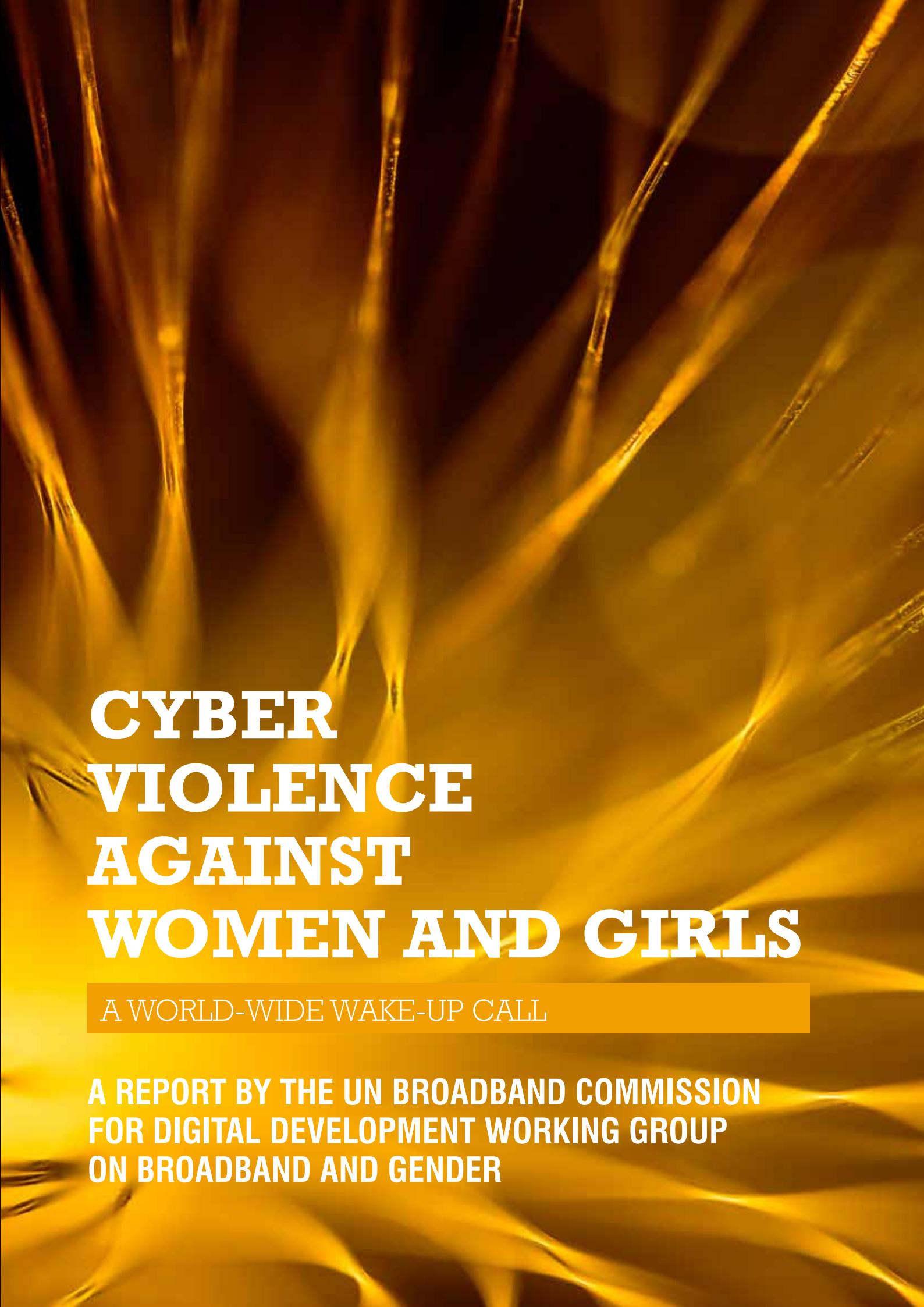


CYBER VIOLENCE AGAINST WOMEN AND GIRLS

A WORLD-WIDE WAKE-UP CALL

A REPORT BY THE UN BROADBAND COMMISSION FOR DIGITAL DEVELOPMENT WORKING GROUP ON BROADBAND AND GENDER

CYBER VIOLENCE AGAINST WOMEN AND GIRLS:

A WORLD-WIDE WAKE-UP CALL

Acknowledgements

This Report has been written collaboratively, drawing on insights and rich contributions from a range of Commissioners and Expert Members of the Working Group on Broadband and Gender. It has been researched and compiled by lead author Nidhi Tandon, assisted by Shannon Pritchard, with editorial inputs by teams from UN Women, UNDP and ITU.

Design concepts were developed by Céline Desthomas of ITU. We wish to thank the following people for their contributions and kind review and comments (listed in alphabetical order of institution, followed by alphabetical order of surname): Dafne Sabanes Plou, Jac sm Kee and Chat Garcia Ramilo (APC); Dr Nancy Hafkin; Minerva Novero-Belec (UNDP); Corat Suniye Gulser (UNESCO); Jennifer Breslin and team (UN Women); Samia Melhem and team (World Bank).

About the Commission

The Broadband Commission for Digital Development was launched by the International Telecommunication Union (ITU) and the United Nations Educational, Scientific and Cultural Organization (UNESCO) in response to UN Secretary-General Ban Ki-moon's call to step up efforts to meet the Millennium Development Goals. Established in May 2010, the Commission unites top industry executives with government leaders, thought leaders and policy pioneers and international agencies and organizations concerned with development.

The Broadband Commission embraces a range of different perspectives in a multi-stakeholder approach to promoting the roll-out of broadband, as well as providing a fresh approach to UN and business engagement. To date, the Commission has published a number of high-level policy reports, best practices and case studies. More information about the Commission is available at www.broadbandcommission.org.

Disclaimer

The opinions, analyses and recommendations contained in this report do not necessarily reflect the views of UN Women, the United Nations Development Programme (UNDP) and its Executive Board, or of the United Nations Member States.

ABBREVIATIONS AND ACRONYMS

APC	Association for Progressive Communications
CEDAW	Committee on the Elimination of all forms of Discrimination Against Women
ICT	Information and Communication Technology
IGF	Internet Governance Forum
ISPs	Internet Service Provider(s)
OSCE	Organization for Security and Co-operation in Europe
PTSD	Post-Traumatic Stress Disorder
SNS	Social Networking Service/Site
UGC	User Generated Content
VAWG	Violence Against Women and Girls

EXECUTIVE SUMMARY

Millions of women and girls around the world are subjected to deliberate violence because of their gender. Violence against women and girls (VAWG) knows no boundaries, cutting across borders, race, culture and income groups, profoundly harming victims, people around them, and society as a whole.[1]

The growing reach of the Internet, the rapid spread of mobile information and communications technologies (ICTs) and the wide diffusion of social media have presented new opportunities and enabled various efforts to address VAWG.[2] However, they are also being used as tools to inflict harm on women and girls. Cyber-VAWG is emerging as a global problem with serious implications for societies and economies around the world. The statistics pose risks to the peace and prosperity for all enshrined in the Charter of the United Nations, and, in particular, to the goals of inclusive, sustainable development that puts gender equality and the empowerment of women as key to its achievement.

Writing this report has, in some sense, been a race to keep up with breaking news, as girl after girl and woman after woman, has come forward to expose physical and verbal attacks on them: teenage girls driven to suicide by *online trolling*; an airline passenger using her cell phone to record and report physical and sexual harassment from a male co-passenger; an actress publicly responding to targeted *online hate speech* against her; a former Major League Baseball pitcher using *doxing*[3] to identify people responsible for "Twitter troll" posts with obscene, sexually explicit comments about his teenage daughter.

A current Twitter hashtag[4] shows just how rough it is being a woman on the Internet in North America. Women of the Global South also experience various acts of cyber VAWG, but these are usually less well-publicized.

High profile incidences attract public attention and tort law responses: aTwitter troll was jailed[5] in September 2014 and a porn site operator sentenced to 18 years in in prison in February 2015[6]. One person was suspended from his community college, and another lost a part-time job with the New York Yankees when the *doxing* case involving a former Major League Baseball pitcher was made public. In May 2015, a Toronto sports reporter was verbally assaulted while broadcasting live at a professional soccer league game. Following public outrage, the main

aggressor lost his high paying job at a public corporation. The sports team also banned four of the offenders from the stadium.

Responses, however, have yet to fully address the many degrees and impact of violence, trauma and loss that women, girls and children are routinely exposed to and that go unreported. It is a problem of pandemic proportion when research asserts[7] that one in three women will have experienced a form of violence in her lifetime. Cyber VAWG could significantly increase this staggering number, as reports suggest that 73% of women have already been exposed to or have experienced some form of online violence[8] in what must still be considered a relatively new and growing technology.

The sheer volume of cyber VAWG has severe social and economic implications for women and girls.[9] Threats of rape, death, and stalking put a premium on the emotional bandwidth and put a stress on financial resources (in terms of legal fees, online protection services, and missed wages, among others). The direct and indirect costs to societies and economies are also significant, as needs for health care, judicial and social services rise and productivity goes down with the sense of peace and security required for business to thrive. Cyber VAGW can also have adverse impact on the exercise of and advocacy for free speech and other human rights.

Perpetrators of VAWG are rarely held accountable in part due to the relatively low capacity to prosecute offenders.

"There is one universal truth, applicable to all countries, cultures and communities: violence against women is never acceptable, never excusable, never tolerable."

United Nations Secretary-General Ban Ki-moon (2008)

Societal barriers, the limitations of legal recourse and other factors hamper access to justice for many women, particularly for girls and women living in poverty. This situation exacerbates already low reporting levels and spiraling a vicious cycle.

In 1995 less than 1 per cent of the world population was connected to the Internet. That number has grown to 40 per cent, with over three billion unique Internet users.[10] While women are about 25 per cent less likely to have access today, Intel's 2013 report, *Women and the Web*, estimates 450 million new female Internet users could come online within the next three years. Another report on women's access to and use of mobile technology shows a growing gender "use" gap which is partly attributable to women's concerns over privacy and security.[11] Given the ubiquity of the Internet and its wide-ranging impact, particularly on the younger generation, it becomes imperative to ensure it as a safe place for both current and future generations.

The respect for and security of girls and women must at all times be front and center of those in charge of producing and providing the content, technical backbone and enabling environment of our digital society. Failure to do so will clip the potential of the Internet as an engine for gender equality and women's empowerment.

The increasing spread of the Internet frames the urgency for effective legal and social controls on attitudes and criminal behavior online. As this paper goes to print, Ellen Pao, former CEO of the online forum Reddit expressed grave concerns about the tensions between balancing freedom of expression with privacy and protection of Internet users.[12] Rigorous oversight and enforcement of rules banning cyber VAWG on the Internet is going to be a *conditio sine qua non* if it is to become a safe, respectful and empowering space for women and girls, and by extension, for boys and men. Governments, regulators,

businesses and everyday netizens alike need to demand and act on the basic principle that an unsafe Internet arena will mean that women will frequent the Internet less freely, with costly societal and economic implications for all.

> "Our work to eliminate violence against women is central to our commitment to promote gender equality and the empowerment of women, both of which are integral to sustainable development."
>
> *Helen Clark, UNDP Administrator, Statement on the International Day for the Elimination of Violence against Women (2014)*

Sensitization, Safety and Sanctions: a way forward

The first imperative in eliminating cyber VAWG is prevention. Changing social attitudes and norms is the first step to shifting the way online abuse is understood as a serious challenge. Violence is not new, but cyber violence is, and the public needs to recognize this and address it as a priority issue. Sensitization to cyber VAWG must include educating the next generation of ICT users, both boys and girls, through their parents, teachers and wider communities, as well as police authorities and the justice systems.

The second imperative is to put in place and implement safeguards to secure safe online spaces. Over the years, traditional VAW safety measures have evolved to include women's shelters, crisis centres, help lines and education. In light of the new cyber VAWG challenge, the digital world also urgently requires safety measures to keep up with a rapidly evolving Internet. This will necessarily require resources, attention and active participation of industry (digital gatekeepers), civil society and governments.

Third in this multi-level approach to addressing cyber VAWG are sanctions, which address laws as well as the will and ability of the courts and legal systems to enforce compliance and punitive consequences for perpetrators. Establishing necessary laws is a starting goal; the next steps should ensure effective implementation. Sanctions however cannot on their own accord, define or set societal norms, or deter unlawful activity, or remedy injuries. The challenge requires a broad-based societal action, engaging all stakeholders. For this reason, while part of the solution, a mere legal reform agenda alone centered on perpetrators or abusers would be limited in both its reach and impact.

Free speech is a fundamental right, and its preservation requires vigilance by everyone. Free speech online requires the vigilance particularly of those who use the Internet. Some suggest that the establishment of a Cyber Civil Rights Initiative (CCRI) through international collaboration is necessary to ensure a safe Internet. Others still stress that international human rights principles already provide the underpinning for a safe Internet, with the Human Rights Council's recognition that human rights apply offline as well as online.[13]

International and national laws and trans-national collaborative alliances are slowly evolving to address common global concerns of cyber VAWG, but if not dealt with commensurate to the challenge, crimes committed are likely to continue to increase, as more of the world goes online and these technologies become more and more a part of everyday life.

Each of the above imperatives of sensitization, safeguards and sanctions supports the others, and will need consistent, collaborative action at many levels. Failure to address and solve cyber VAWG could significantly impede the digital inclusion of women everywhere, putting women at increasing disadvantage for being excluded from enjoying the benefits of ICTs and the Internet.[14]

"… the landscape of gender-based violence has been transformed … [but] rather than there being a dramatic reduction in violence against women, … the challenges have become more complex, the resistance to change deeper, the backlash against the empowerment of women more blatant and the methods used to uphold the status quo more sophisticated and insidious."

UN Women (OSCE, 2009)

Readers might broadly agree that society's failure to address gender-based violence and crimes is symptomatic of a wider social failure to respect and honor each other regardless of sex, age, creed or race. "Culture is the sphere where we socialize ourselves – and the Internet- global in its reach, is a dimension of that sphere".[15]

As the Internet evolves and social media and networking tools increasingly become an intrinsic part of people's lives around the globe, attitudes and norms that contribute to cyber VAWG must be addressed with urgency. A collective global effort, led by the United Nations system, has put in place the pillars for a 21st century sustainable development paradigm. The Sustainable Development Goals (SDGs) establishing the global development priorities for the next 15 years includes a goal on gender equality, which places women's access to technology for their empowerment as one of the core indicators for progress. For this to be realized, all stakeholders must take accelerated actions to ensure a safer, more secure Internet for present and future generations – one without endemic VAWG.

1

WHY THE BROADBAND COMMISSION FOR DIGITAL DEVELOPMENT NEEDS TO LEAD ON CYBER VIOLENCE AGAINST WOMEN AND GIRLS

1.1 Cyber-VAWG is a systemic societal concern and challenge

Almost without exception, across national boundaries and jurisdictions, millions of girls and women are subjected to deliberate forms of violence because of their gender. The violence includes dehumanizing, aggressive and harmful acts that are in turn physical, psychological, sexual, and exploitative. These acts take place behind closed doors in the privacy of homes or workplaces, out in the open in public settings, and sometimes in the midst of communities and societies (such as the mob lynching of women, reported femicide[16] and the sex and human trafficking trades). The systematic targeting of girls and women is also a tactic used in war and conflict.[17]

Sexual harassment and domestic violence were broadly accepted as personal practices and private relational concerns up until four decades ago. Throughout the 1970's and 80's, civil rights activists campaigned to have these *private affairs* and *cultural practices* recognised and treated as harmful societal problems.[18] As the table below illustrates, the United Nations (UN) acknowledged the issue in the early 1990's. Twenty-five years later, however, efforts to address violence against Women (VAW) and

issues of prevention, redress and services, remain in need of substantive resources and concerted and coordinated efforts across societies and sectors – including government and non-governmental organizations, policy makers, law enforcement bodies, social service agencies, educators, journalists, trade unions, international organizations, donors, and the entire Internet community.

Cyber VAWG includes hate speech (publishing a blasphemous libel), hacking (intercepting private communications), identity theft, online stalking (criminal harassment) and uttering threats. It can entail convincing a target to end their lives (counselling suicide or advocating genocide). The Internet also facilitates other forms of violence against girls and women including trafficking and sex trade. Not only does commercialized sex on the Internet drive the demand for the sex industry overall, it also allows traffickers to use the legal aspects of commercial sex on the Internet as a cover for illegal activities. Some of the main uses of the Internet by traffickers include: advertising sex, soliciting victims on social media, exchanging money through online money transfer services, and organizing many of the logistical operations involved in transporting victims.[19]

In May 2013, the Broadband Commission agreed to an ambitious new target designed to spur female access to ICT, calling for gender equality in broadband access by the year 2020. The goal is to use ICT to transform the lives of millions of women by giving them access to, inter alia, life-enhancing health, education, opportunities for income generation, access to services, avenues for political participation and mobilization.[20] The use of ICTs also extends to preventing and responding to violence against women but this use also depends on the internet serving as a safe and welcome place for women. Therefore, this report serves to address a critical issue in determining whether the gender goals of the Broadband Commission are achieved.

In the age of the social Internet,[21] networks of networks of 'distributed intelligence' and accessible mobile platforms are spanning out to ever more remote corners of the world. Digital 'platforms' for violence can now instantly transmit, across time and space, to billions of people: creating new and false realities, feeding grounds and challenges for both perpetrators and targets. Unchecked, this behaviour runs the risk of producing a 21st century global pandemic with significant negative consequences

Broadband Commission Working Group on Gender Objectives for Digital Inclusion:

- Promote digital inclusion for women
- Empower women through digital literacy training and skills building
- Promote the development of gender-sensitive applications (monitor violence against women, etc.) in partnership with the private sector and civil society
- Foster public service delivery which takes into account the specific needs of women and their surroundings
- Make technology training and jobs more attractive to girls and women
- Promote digital entrepreneurship among women to foster social innovation
- Foster the protection of girls and women when they go online
- Contribute to the post-2015 development agenda

"Gender inequality and discrimination are root causes of violence against women, influenced by the historical and structural power imbalances between women and men which exist in varying degrees across all communities in the world."

Source: UN Women

for all societies in general and irreparable damage for girls and women in particular.

An emerging set of anti-social, aggressive and violent content and behaviours are available to anyone who logs on to the Internet, regardless of age, gender, culture or values. Mobile Internet access means these can come at any time, and can follow their targets everywhere. The growing ubiquity of mobile devices means those targeted or indirectly implicated are getting younger and younger — with children as young as 5 or 6 years of age now exposed to cyber bullying and online pornography — sometimes of the most extreme kind. In some contexts online culture represents the worst form of gang violence.

Online crimes are not a 'first world' problem; they seamlessly follow the spread of the Internet. The use of WhatsApp instant messaging, for example, has become, according to some reports, the latest harassment tool of choice in countries like India and Malaysia, and increasingly around the world. Pornographic imagery produced in one country now lands in the hands of anyone anywhere. This is not to say that WhatsApp is not a positive and useful tool. Many women and men use the app for activism — and netizens use it simply to communicate.

Violence online and offline, or 'physical' VAWG and 'cyber' VAWG, feed into each other. Abuse may be confined to networked technologies or may be supplemented with offline harassment including vandalism, phone calls and physical assault. Similarly, the viral character of distribution is now explosive. What was once a private affair can now be instantly broadcast to billions of people across the digital world.

There is a well-worn statistic that 30% of all Internet traffic constitutes porn: Research also reveals that 88.2% of top rated porn scenes contain aggressive acts and 94% of the time the act is directed towards a woman.[22] Furthermore,

"We hear about wake-up calls, but people keep hitting the snooze button."

Ira Winkler
President of the Information Systems Security Association

studies show that after viewing pornography men are more likely to: report decreased empathy for rape victims; have increasingly aggressive behavioral tendencies; report believing that a woman who dresses provocatively deserves to be raped; report anger at women who flirt but then refuse to have sex; report decreased sexual interest in their girlfriends or wives; report increased interest in coercing partners into unwanted sex acts. Boys aged 12-17 are the largest consumer group of Internet porn.[23] This suggests that the first images and information surrounding sex that a young boy is exposed to would include violence towards a woman.

The key is to focus on prevention, particularly among young children, and on developing an array of strategies to address VAWG. These could include education programs targeting primary-age children, after-school and community-based programs for youth, employment training programs, and support and effective and sustainable funding for positive and expressive outlets such as sports, art and music. From an industry point of view, there is a preventative as well as a proactive set of measures that can be taken to complement these actions.

The social and structural inequalities contributing to VAWG are well established and recognized within normative frameworks such as CEDAW and the recent Istanbul Convention. UN Women provides the following recommendations[24]:

- Investing in gender equality and women's empowerment
- Introducing or reforming legislation

Acknowledging VAW is a relatively recent development. Highlights of key international and regional commitments and campaigns over the past century include:

Early 20th century

Trafficking and sexual exploitation identified as a concern within international conventions.

1979

The Convention on the Elimination of all Forms of Discrimination Against Women or CEDAW was adopted (entered into force in 1981) and its Optional Protocol (2000).

1993

The landmark Declaration on the Elimination of Violence against Women (1993) was adopted, providing a framework for analysis and action at the national and international levels.

1994

Inter-American Convention on the Prevention, Punishment and Eradication of Violence against Women (Convention of Belém do Pará) was adopted. It is the first and only legally binding instrument at the regional level on violence against women.

- Ensuring holistic multi-sectoral policies and national plans of actions
- Securing resources/gender-responsive budgeting
- Promoting primary prevention
- Main strategies and lessons learned for key sectors
- Developing coordinated community responses
- Engaging key groups
- Capacity development
- Conducting research, data collection and analysis
- Monitoring and National Accountability

All the platforms used to commit cyber VAWG have to be understood and addressed in the context of multiple trends in social violence, whether committed on the streets in communities or in the homes of families; whether disseminated by the traditional media or the Internet writ large.

1.2 The time to act is now

The use of computers and information technologies for criminal and abusive activity is not a new phenomenon.[25] So what has changed? To some extent, the issue has been brought to the fore by heightened public awareness promoted by media sensationalism, high-profile stories, and the sense that the online bully is for all intents and purposes immune to accountability of any form. In the last two decades, violence has spread onto virtual platforms and online spaces, where the Internet globalizes, facilitates and compounds its impact.[26]

The communication tools offered by new technologies are being misused by both men and women to assert dominance, to manipulate, to terrorize, to humiliate, and to silence. The Internet clearly facilitates acts of violence, sexual and other offences both online and off-line, and provides easy access to victims for trafficking and other

1999	2008	2010	2013
25th November was designated United Nations International Day for the elimination of violence against women.	The United Nations Secretary-General launches an unprecedented global campaign, UNiTE to End Violence against Women.	The Secretary-General appoints a Special Representative on Sexual Violence in Conflict and the Human Rights Council adopted Resolution 14/12 on accelerating efforts to eliminate all forms of violence against women.	Member States adopt agreed conclusions during the 57th Commission on the Status of Women on the prevention and elimination of all forms of violence against women.

For a complete timeline see :
http://www.endvawnow.org/en/articles/302-timeline-of-policy-commitments-and-international-agreements-.html?next=303

"For women, the basic problems are the problems that are much larger than technology. They are the gender equality, the patriarchy, the violence against women who dare to use the technologies because men are suspicious. The forces that keep women and girls from going to school. These forces keep them from using the technology—even if it is in the house."

Nancy Hafkin, Senior Associate, Women in Global Science and Technology

The 5 P's of Due Diligence

1. Prevent violence against women
2. Protect women from violence
3. Prosecute and investigate incidences of violence against women
4. Punish perpetrators of violence against women
5. Provide redress to victims/survivors of violence against women

Due Diligence Project

forms of exploitation. Underlying this is the perpetuation of negative and harmful stereotypes of girls and women as well as negative notions of masculinity.

The potential to broadcast cyber-violence and hate crimes against women is particularly noticeable; it is exponential, unprecedented and at times corrosive and vitriolic, and it represents the very worst of mob mentality and perceived 'safety in numbers' by the perpetrators. Online harassment has become, in part, a team sport, with posters vying to outdo each other. Compared to men, women who are active on social media and in the blogosphere receive more threats or comments that directly attack their gender, their safety, and their very right to express opinion in male-dominated spaces.[27]

1.3. Objectives and limitations of this report

Gender-based violence has multi-dimensional social expressions and implications and is seemingly chronically endemic to human civilisation. Others have weighed in on this issue, to give both space and voice to them all would go beyond the objective and scope of this paper. While the cyber manifestations of VAWG is not an issue of importance 'only' to girls and women – this paper focuses on girls and women as a particular segment of society that has been especially targeted because of its societal status. Society as a whole has a poor track record of addressing harms primarily suffered by females. The injustice of rape, for example, is compounded by the injustice of official neglect and indifference.[28]

The main objectives of this paper are to:

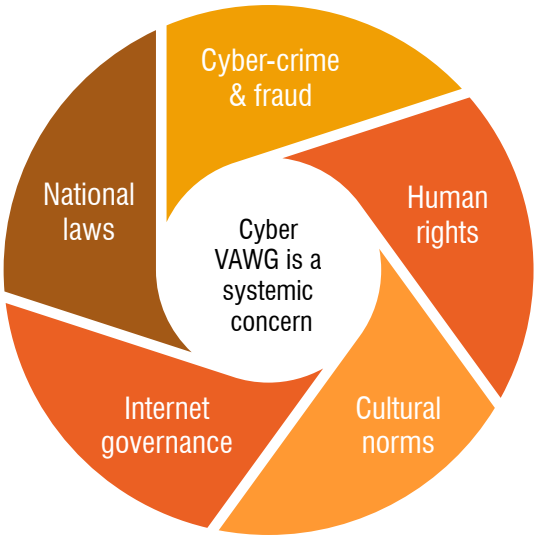
- situate the growing threat of cyber VAWG within the broader context and challenge of cyber-crime, Internet growth and governance, and human rights;

- define key priority areas of action that address the 5Ps of Due Diligence, through public sensitization, compliance of safeguards and the implementation of sanctions.

The paper highlights the need for change on all levels, and seeks to:

- frame these societal concerns, their ramifications and impacts in relation to guiding public perception, user behaviour from the end user point of view;
- postulate the necessary policy guidelines and frameworks around Internet governance for industry and service providers;
- join others in raising the alarm and driving an urgent call for concerted and coordinated action on multiple fronts, through sensitization, safeguards and sanctions.

The objective is not to 'drive' perpetrators and predators further underground (into the Undernet for instance), but to complement punitive systems and law enforcement with incentives to change behaviours through prevention, advocacy, education and the equivalent of 'neighbourhood watch' in the form of online civil society activities. The graphic provides a high-level view of the complexity and interdependence of issues in dealing with cyber VAWG.



The **Due Diligence** project has evolved from CEDAW (1979 and 1993) and seeks to advocate for the inclusion of the 5Ps in VAWG discourse globally. It demands that States focus on unequal gendered structures and the wider social, economic and political environment in which gender discrimination thrives. The Due Diligence Framework and its Guiding Principles assist in identifying the different actors, stakeholders, and allies; take into account the socio-economic-historical contexts of women and particular groups of women; and emphasize the need to address root causes, risk factors and incorporate transformative justice ideals into programmes, laws and policies to eradicate discrimination against women.

2

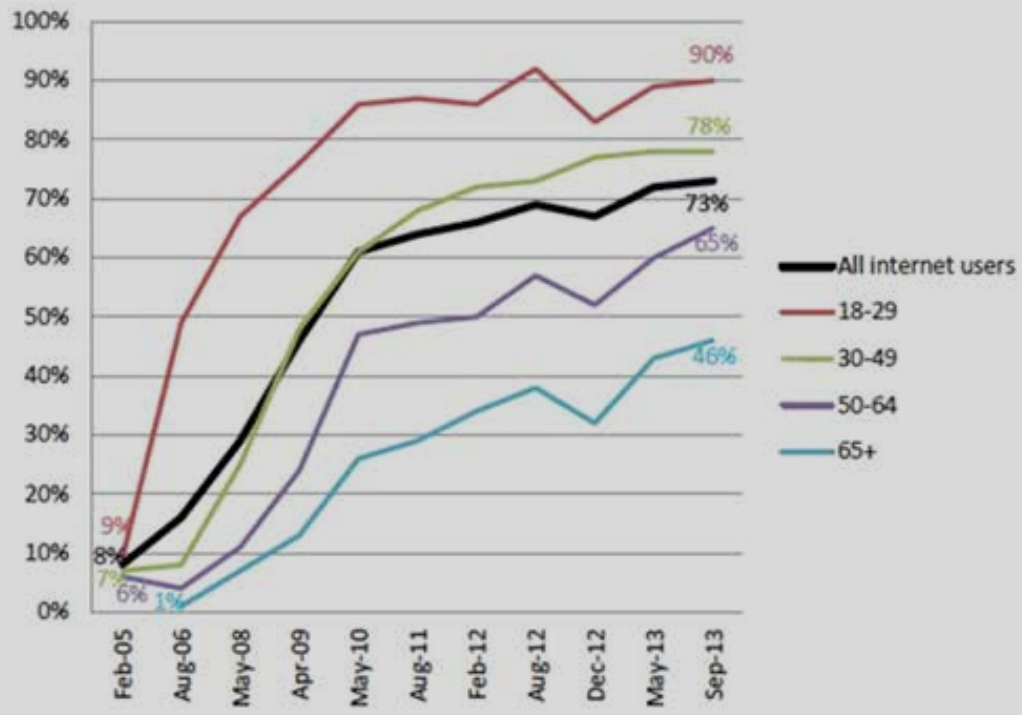
THE EVOLUTION OF THE INTERNET AND ITS RAMIFICATIONS FOR 'CYBER VAWG'

2.1 What the numbers tell us

Violence against women

- Violence against women has been described as a 'pandemic 'in Europe, where 62 million women, or one in three, have suffered from violent acts since the age of 15. This pandemic is very much evident around the globe. It has manifested itself on a disturbing scale in many countries, in some parts 8 out of 10 women are reported to suffer some kind of violence including sexual, physical and psychological violence.[29] The prevalence of intimate partner violence alone can range between 15 and 71 percent measured comparatively in different countries. This tells us there is nothing inevitable about violence against women and girls; its levels and dynamics are not fixed and can be altered – and governments, organizations, communities and individuals can make a difference.[30]
- In 2014 the *European Union Agency for Fundamental Rights* (FRA) published the results of a survey on VAW suffered in their families, at work, in public and on the Internet as well as the effect it has on their lives and the way in which victims respond to aggression. Surprisingly the

> "Until domestic violence became a national policy priority, abuse was dismissed as a lovers' quarrel. Today's harmless jokes and undue burdens are tomorrow's civil rights agenda."
>
> *Amanda Hess, Technology Journalist*



Source: Latest data from Pew Research Center's Internet Project Library Survey, July 18 - September 30, 2013. N5, 112 intenet users: age 18+. Interviews were conducted in English and spanish and on landline and cell phones. The margin of error for results based on internet users

Social networking site use by age group, 2005-2013

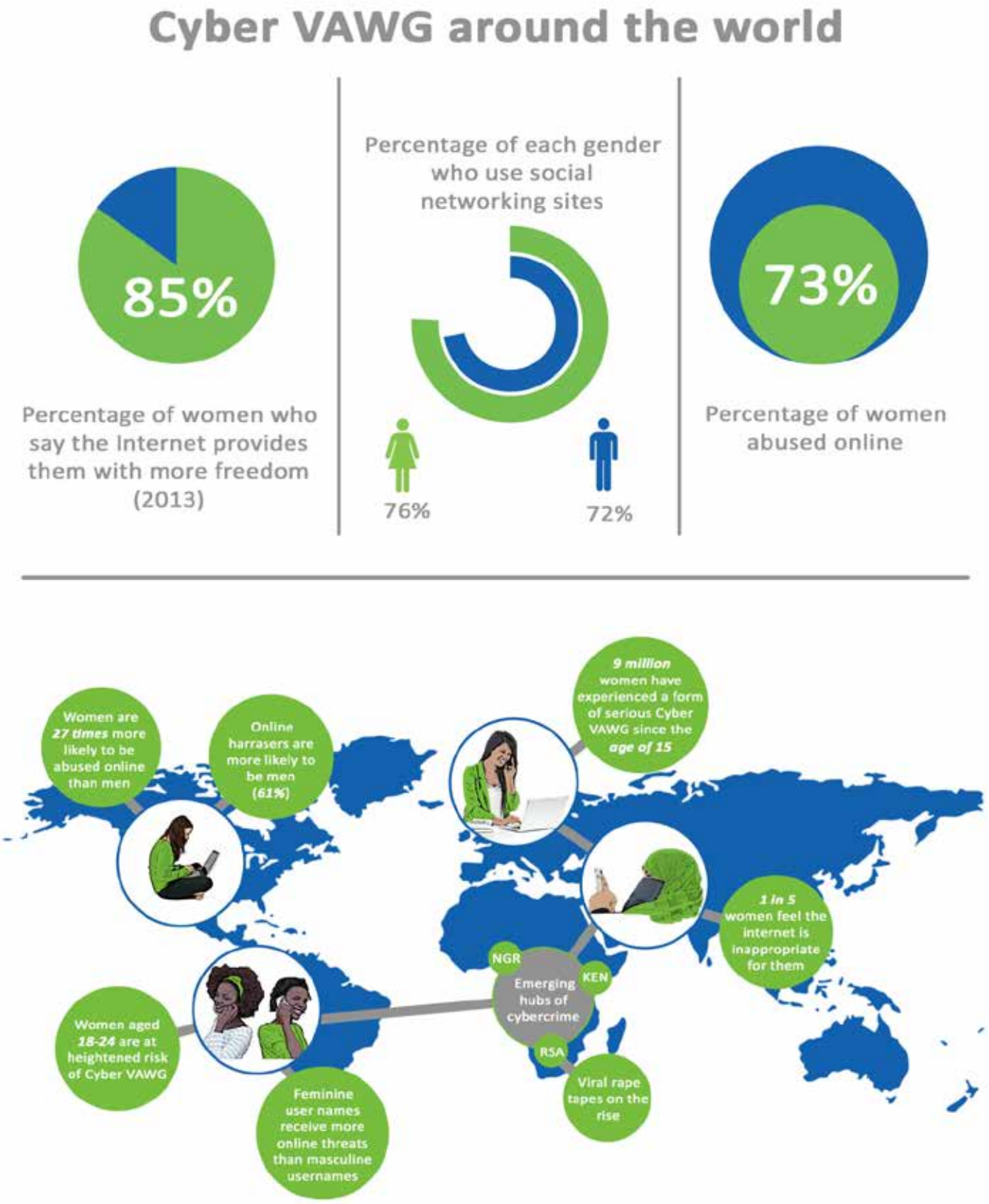
% of internet users in each age group who use social networking sites, over time

countries with the highest percentage of victims of violence against women are in northern Europe: Denmark (52%), Finland (47%) and Sweden (46%), while Hungary (21%), Austria (20%) and Poland (19%) have much lower rates.

- Non-fatal acts of violence take a particular toll on women and children. One in four children has been physically abused; one in five girls has been sexually abused; and one in three women has been a victim of physical and/or sexual intimate partner violence at some point in her lifetime.[31]

Access

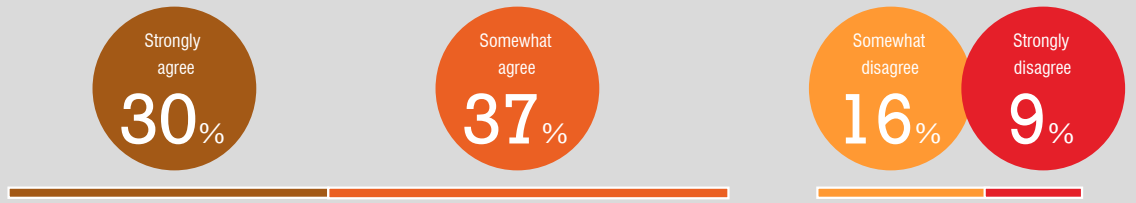
- Close to four billion people now use the Internet. China has the most users (642 million in 2014) comprising nearly 22 per cent of the world's total. Among the top 20 countries, India has the lowest penetration rate; a mere 19 per cent, but commands the highest yearly growth rate. In the United States, Germany, France, U.K., and Canada over 80 per cent of population have an Internet connection.[32]
- The use of smartphones – which give mobile web access – is significant. A 2014 report from eMarketer suggests 1.76 billion people owned a smartphone, up 25 per cent over 2013; "…by 2017, more than a third of all people around the globe will be smartphone users."[33] The impact is projected to be dramatic as access is expected to enable people, including those from low-income countries, to use, generate, and contribute to spread of information at an unprecedented rate.



Source: Networked Intelligence for Development 2015

Opinions on the Internet "Agree" vs "Disagree"

Average of 17 Countries, 2014



The internet gives me a greater freedom

The internet is a safe place to express my opinions

The white space in the charts represents "Depends"and "Don't know"

Asked of half samples

Source: 2014 BBC World and GlobeScan poll

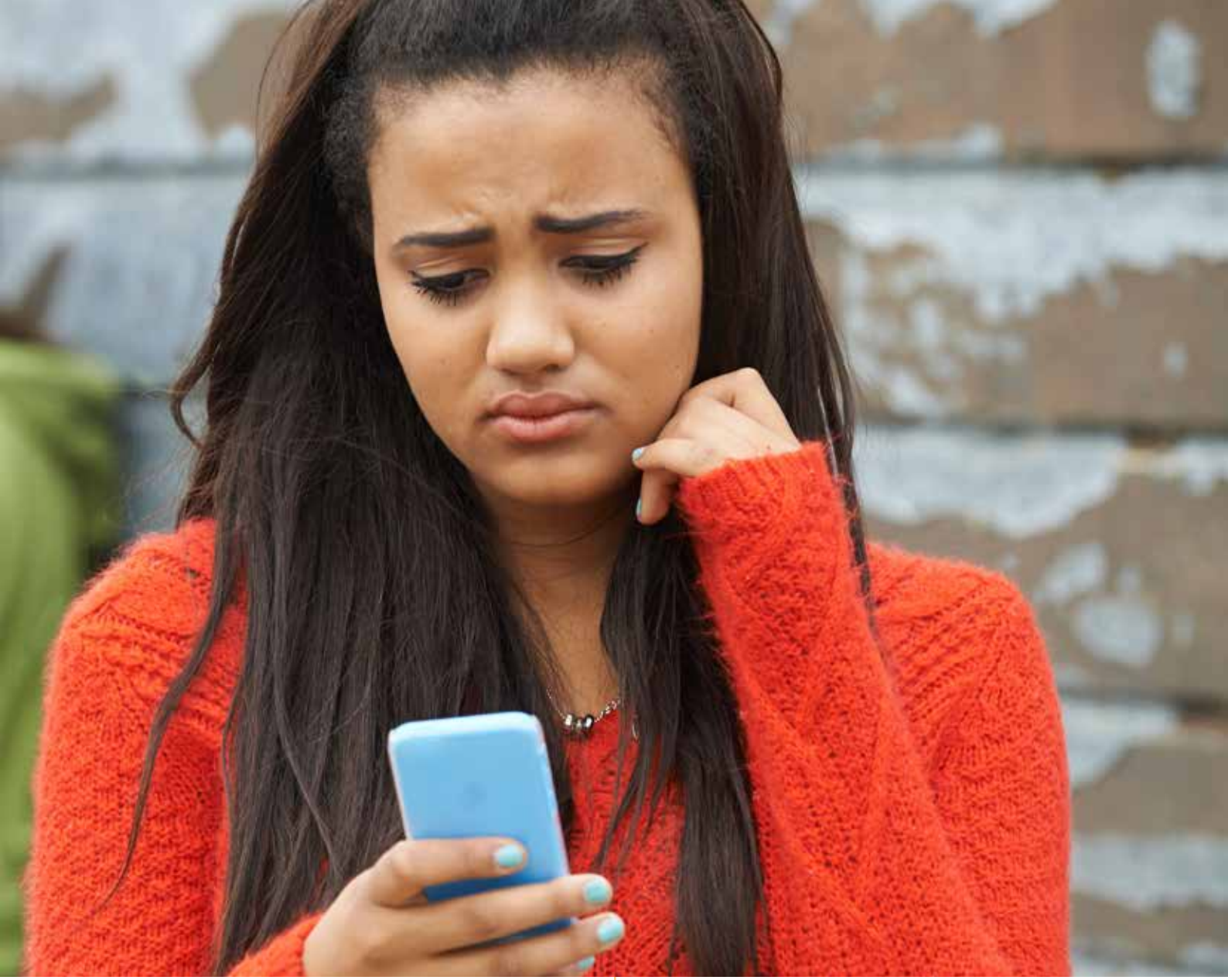
- More women play video games than ever before, but women who talk about video games on social media face criticism, harassment, even threats, while men largely don't.[34] The Internet Advertising Bureau reported in October 2014 that 52% of the gaming audience is made up of women.[35]
- According to a Pew Research Center survey conducted in January 2014, 74 per cent of online adults in the United States use social networking sites; 76 per cent of total SNS users are women compared with 72 per cent of men.[36]

As the 'social Internet' continues to grow exponentially, it has becomes almost impossible to monitor and control illegal and harmful content. To understand the magnitude, some data references are helpful. As of the first quarter of 2015:

- Facebook had 1.44 billion monthly active users.[37] This translates to 50 per cent of Internet users worldwide.[38]
- YouTube reported over 72 hours of video uploaded every minute[39]
- Twitter averaged 236 million monthly active users.[40]
- Some 500 million people use mobile devices and the WhatsApp mobile text messaging application.[41] In India alone WhatsApp users reached 70 million per month.[42]

Cyber-Violence

- Women aged 18 to 24 are at a heightened risk of being exposed to every kind of cyber VAGW; they are "uniquely likely to experience stalking and sexual harassment, while also not escaping the high rates of other types of harassment common to young people in general", like physical threats.[43]
- In the EU-28, 18 per cent of women have experienced a form of serious Internet violence since the age of 15, which corresponds to about 9 million women.[44]



These figures do not tell the entire story however. Kenya's office of the Director of Public Prosecutions acknowledges that women who are victims of cybercrime and bullying very rarely report the crime.[45] A report from India, for instance, suggests that "only 35 per cent of the women have reported about their victimization, 46.7 per cent have not reported and 18.3 per cent have been unaware of the fact that they have been victimized … women prefer not to report about their victimization owing to social issues." [46]

As the ease of connectivity increases worldwide, so will the reach of violence. These statistics underpin the urgent need to ensure a safe Internet for all.

2.2 How the Internet is perceived – trust, safety and freedom

- A 2014 BBC World and GlobeScan poll across 17 countries – in both developed and developing countries – revealed a growing sense of insecurity among users. GlobeScan's Chair commented that: "The poll suggests that two of the underpinnings of modern democracies are at risk – a media seen as free and fair; and an Internet safe for the free expression of views."
- Those who feel "the Internet is a safe place to express opinions" (40 per cent) are outnumbered only slightly by those who disagree (52 per cent).

France is among the countries where respondents do not feel they can express their opinions safely online (76 per cent), alongside South Korea (72 per cent), Spain (66 per cent), Canada, the USA, and Germany (65 per cent each). Only six surveyed countries have majorities that feel they can express their opinions online safely: Nigeria (71 per cent), India (67 per cent), Indonesia (57 per cent), Kenya (52 per cent), Pakistan and Peru (both 51 per cent) – all of them emerging or developing countries.

- At the same time, two-thirds of respondents (67 per cent) say the Internet brings them greater freedom, with the most enthused respondents being in Africa (81 per cent in Nigeria and 78 per cent in Kenya), followed by Australians (77 per cent), Britons (76 per cent), Indonesians (73 per cent), Canadians and Americans (both 72 per cent). In contrast, people in China do not report a strong sense of increased freedom from using the Internet, with a narrow majority agreeing with the statement and 45 per cent disagreeing with it.
- The counter-evidence shows that 70 per cent of Internet users consider the Internet to be 'liberating' and in a 2013 survey of 2,200 women; 85 per cent said it "provides more freedom."

If the Internet continues to be an arena where users can be harassed, stalked, bullied and threatened with impunity, the 'liberating' and 'safe' aspects of this space will inevitably shrink. This could turn away existing and potential new users. It is already turning away women as noted in a recent GSMA report

GSMA: Bridging the gender gap: Mobile access and usage in low- and middle-income countries, 2015

UN Women and Microsoft under the UN Women Safe Cities programme developed a methodology to fill a knowledge gap around access to and use of mobile phones to address violence against women and girls, particularly in public spaces in disadvantaged areas in the city. The findings from Delhi, Marrakesh and Rio studies provide nuance and insights around these issues, as well into the challenges with online violence against women and the potential and barriers to the use of mobile technology to combat violence against women and girls in cross-regional perspective. The full city reports also detail the local context, issues, potential and benefits of mobile phones for addressing girls' and women's public safety concerns. The following box provides highlights of some of the threats and barriers, as well as steps to overcome them.

Mapping Access to and use of Mobile Phones to Document, Prevent and Respond to Sexual Violence against Women and Girls in Urban Public Spaces:

Findings from 3 Qualitative Methods Studies in the Low-income Communities in the Cities of Marrakech, New Delhi and Rio-de-Janeiro

UN Women Global Safe Cities Initiative, with support from Microsoft

Benefits of Mobile Phones for Women's Public Safety

- On the whole women feel safer with a mobile phone

Challenges to Use, Confidence and Safety Concerns

- Many women and girls in the low-income communities have access to the basic mobile phones, without connection to Internet (which makes Internet-based safety applications unusable for them)
- Fluidity of mobile phone ownership (e.g. phone sharing) and related issues of privacy
- Girls' and women's control of phones and use more limited (e.g. access and ability to pay for services and features used, intra-household decision-making)
- Fear of online environment, tracking and some mobile phone features (e.g. camera) as a barrier to use. This fear can be real, perceived or used as a scare tactic to dissuade women from going online.
- Lack of sophistication of use of mobile phones that prevent girls and women from understanding and managing their online presence
- Lack of awareness of empowerment dimension of internet and through mobile phone use
- Lack of use of phones to document and report VAW due to fears of being tracked, re-victimization, and lack of trust in authorities and wide spread victim/survivor blaming

Recommendations

- Improve girls' and women's access to affordable and accessible (e.g. for low literacy levels) mobile technology, services and data plans including affordable mobile devices with internet connectivity (feature and smart phones).
- Address issues of awareness of tools and services online and digital literacy and training for girls and women
- Adopt laws to regulate internet based crimes related to VAW online and address other intuitional needs like public review mechanisms, and training within the justice and police system
- Increase girls' and women's self-awareness about what constitutes VAW online and awareness of rights, and develop public campaigns on violence against women (online and off)
- Increase understanding around how privacy affects girls' and women's use of mobile phones
- Safety and privacy audits of apps to prevent risks and increase confidence in use
- Develop technology solutions to protect girls' and women's privacy
- Engaging girls and women as content creators and developers of solutions, including those around combatting VAW and also addressing gaps in solutions (e.g. around prevention)
- Tackle hand in hand all the offline challenges around VAW and gender norms
- Collect gender-disaggregated data on access to and use of technology

3

DEFINING THE THREAT ENVIRONMENT: THE 'CYBER' NATURE OF VAWG

3.1 Terminologies, definitions and trends

The United Nations 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."[48] It includes forced intimate partner violence and sexual assault, marriage, dowry-related violence, marital rape, sexual harassment, intimidation at work and in educational institutions, forced pregnancy, forced abortion, forced sterilization, trafficking and forced prostitution and gender-related killings.

The term 'cyber' is used to capture the different ways that the Internet exacerbates, magnifies or broadcasts the abuse. The full spectrum of behaviour ranges from online harassment to the desire to inflict physical harm including sexual assaults, murders and suicides.[49] Cyber violence takes different forms, and the kinds of behaviours it has exhibited since its inception has changed as rapidly — and, unchecked, will continue to evolve — as the digital and virtual platforms and tools have spread.

> "The widespread circulation of such content is particularly harmful for women. The pervasive gender discrimination in our society is further heightened since the digital medium provides the convenient shield of anonymity and fake identities. Errant persons become more emboldened in their offensive behavior since it is presumed that they will not face any consequences."
>
> *K. G. Balakrishnan, former Chief Justice of India*

"The Internet is a forum where perpetrators of these crimes feel a sense of unaccountability for their actions and as such can create a climate in which women do not feel safe or supported."

Rachel Griffen, Director, Suzy Lampugh Trust

According to the VAW learning network, there are six broad categories that encompass forms of cyber VAWG.[50]

1. Hacking: the use of technology to gain illegal or unauthorized access to systems or resources for the purpose of acquiring personal information, altering or modifying information, or slandering and denigrating the victim and/or VAWG organizations. e.g., violation of passwords and controlling computer functions, such as freezing the computer or logging off the user
2. Impersonation: the use of technology to assume the identity of the victim or someone else in order to access private information, embarrass or shame the victim, contact the victim, or create fraudulent identity documents; e.g., sending offensive emails from victim's email account; calling victim from unknown number to avoid call being blocked
3. Surveillance/Tracking: the use of technology to stalk and monitor a victim's activities and behaviours either in real-time or historically; eg. GPS tracking via mobile phone; tracking keystrokes to recreate victim/survivor's activities on computer
4. Harassment/Spamming: the use of technology to continuously contact, annoy, threaten, and/or scare the victim. This is ongoing behaviour and not one isolated incident; e.g., persistent mobile calls/ texts; filling up voicemail with messages so no one else can leave a message
5. Recruitment: use of technology to lure potential victims into violent situations; e.g., fraudulent postings and advertisements (dating sites; employment opportunities); traffickers using chat rooms, message boards, and websites to communicate/advertise
6. Malicious Distribution: use of technology to manipulate and distribute defamatory and illegal materials related to the victim and/or VAWG organizations; e.g., threatening to or leaking intimate photos/video; using technology as a propaganda tool to promote violence against women.

In addition, the proliferation of online violence means cyber VAWG now has its own set of terminology; 'revenge porn'[51] consists of an individual posting either intimate photographs or intimate videos of another individual online with the aim of publicly shaming and humiliating that person, and even inflicting real damage on the target's 'real-world' life (such as getting them fired from their job). This is also referred to as non-consensual pornography. One aspect of 'sexting' is the posting of naked pictures and sending them usually via text messaging. Bluett-Boyd notes that "there is a gendered expectation for girls to provide nude images that draws on already existing social norms and scripts about heterosexuality, male entitlement and female attractiveness." Girls' photos also tend to travel further than the intended recipient and girls experience more social consequences for sexting.

1. 23.3 per cent of women in an online survey reported being blamed for the violence done to them. One woman writes, "most people blamed me for the abuse saying I deserved it. Others ignored it", and another responded, "no help no support at all. I was told that being online is a risk and if I'm being harassed it's my own fault".[52]
2. The anonymity that the Web affords allows pimps to violate laws prohibiting sexual exploitation and violence with impunity, particularly in countries

with strong non-regulation policies. According to Hughes this "mainstreaming of pornography does not mean that the exploitation or abuse of women used in making the pornography has decreased."[53] Instead, as a result of competition among sites, the percentage of violent, misogynistic images has been steadily increasing. Sites are attempting to lure customers with increasingly graphic images. "What is new is the volume of pornography that is being made and that the average person with a computer, modem, and search engine can find more violent, degrading images within minutes than they could in a lifetime 15 years ago." The anonymity of the web can also be used as an advantage to combat cyber VAWG.

3. In the last ten years, some American and European pornography producers have moved to places such as Budapest, Hungary because of the availability of cheap actors from Eastern and Central Europe. Budapest is also a destination and transit city for women trafficked from Ukraine, Moldova, Russia, Romania, and countries of the former Yugoslavia. The city is also now the biggest center for pornography production in Europe, eclipsing traditional centres such as Amsterdam and Copenhagen.[54]
4. In 2014 a virtual market was uncovered involving four websites, online forums and some 30 groups on a popular Chinese messaging platform, connecting traffickers with potential buyers. Some 200,000 boys and girls are kidnapped in China every year and sold online.[55]

3.2. Characteristics and profiles of cyber VAWG

Voices from Digital Spaces: Technology Related Violence against Women identifies five characteristics[56] that distinguish cyber VAWG.

ANONYMITY

abusive person can remain unknown to victim/ survivor

ACTION-AT-A-DISTANCE

abuse can be done without physical contact and from anywhere

AUTOMATION

abusive actions using technologies require less time and effort

ACCESSIBILITY

the variety and affordability of many technologies make them readily accessible to perpetrators

PROPAGATION AND PERPETUITY

texts and images multiply and exist for a long time or indefinitely

Indeed, we are witnessing a broader pool of perpetrators and targets, more and more advanced platforms that broaden scope for surveillance, abuse, storage, difficulty in tracking and catching predators, crossing national boundaries, and faster dissemination and propagation of illegal content. There are profound changes to privacy dynamics and the ability to erase unwanted content.

When UN Women's Ambassador Emma Watson launched the HeforShe campaign and spoke up for feminism, gender equality and challenging gender norms — both masculine and feminine — she was met by online attacks

BOX 1:
RECENT CYBER VAWG TARGETS

Victim	Case details and type of Violence	Age of victim	Location	Date
Amanda Todd school girl	Cyber bullying, including sexual exploitation that led to her taking her own life.	13	Canada	2012
Blandine[1] school girl	Victim of child pornography – naked pictures were posted on a friend's website leading to humiliation and ostracization in her village. Blandine and family did not approach Facebook because they were unaware of a procedure for reporting abuse to an intermediary	15	Democratic Republic of Congo	2013
Rehtaeh Parsons school girl	Gang raped by classmates and photographed. Photos were distributed and Rehtaeh became the subject of mockery and victim-blaming by the community at large. Committed suicide	15	Canada	2014
Anna Mayer Graduate student & journalist	Cyber stalking - sexist trolling	20	USA	2008
Emma Holten Photojournalist	Non-consensual pornography/revenge porn/ hacked photos. Harrassment has continued since 2011	23	Denmark	2011
Peng Hsin-yi TV personality and model	Cyber bullied	24	Taiwan	2015
Zoe Quinn video game developer and 2D artist	A target of Gamergate, suffered harassment including doxing, rape threats, and death threats. In January 2015, Quinn co-founded Crash Override, to help victims of online harassment	28	USA/Canada	2014

Victim	Case details and type of Violence	Age of victim	Location	Date
Marta[2]	Victim of technology-based violence as revenge for her decision to end her marriage. Her US-based ex-husband used fake Facebook and Twitter accounts. Marta highlights the fact that intermediaries' policies on gender violence are not clear and were of no help in her attempts to have the false pages taken down.	32	Colombia	2013
Anita Sarkeesian feminist public speaker, media critic and blogger/ founder of Feminist Frequency	Endured a campaign of sexist harassment including rape and death threats, personal webpages and social media were hacked, and personal information was distributed. She was sent images of herself being raped by video game characters. Also a target of Gamergate.	33	Canada/USA	2013
Ashley Judd actor	In response to tweets about NBA March Madness, Judd received death and rape threats	47	USA	2015
Stella Creasy UK Labor MP and Caroline Criado-Perez – journalist	Sustained social media harassment, which led to changes to Twitter rules	38 & 32	UK	2014
Serena[3]	Public violence of a fake Facebook profile by an ex-husband	64	Bosnia and Herzegoniva	2013

1 http://www.genderit.org/sites/default/upload/case_studies_rdc2_1.pdf
2 http://www.genderit.org/sites/default/upload/case_studies_col4_1.pdf
3 http://www.genderit.org/sites/default/upload/case_studies_byh1_1.pdf

and harassment. This included threats to leak nude photographs of her in an attempt to humiliate her. Though a hoax, the threat still exists and acts like these can serve as silencing mechanisms for young women around the world. In contrast to this type of attitude and behaviour, the HeforShe campaign has shown the commitment of hundreds of thousands of men to speak out against such misogyny.[60]

Other global incidences can be found within the APC report "Cases on women's experiences of technology-related VAW and their access justice".

3.3. Cyber VAWG against the backdrop of cyber-crime

How should cyber VAWG action be integrated with national and international action in the context of cybercrime? According to cyber security industry 2013 survey findings: the cybercrime threat environment has become increasingly pervasive and hostile — and actions to stem the tide of attacks have had limited effect. Digital attack vulnerability is also on the rise: collaboration, expanding the use of mobile devices, moving the storage of information to the cloud, digitizing sensitive information, moving to smart grid technologies, and embracing workforce mobility alternatives without first considering the impact these technological innovations have on their cybersecurity profiles.

Africa has not been immune to increased cybercrime, with countries such as Nigeria, Kenya and South Africa fast becoming hubs of cybercrime activity. New concerns have emerged about technology-facilitated gender-based violence. Currently, mobile phones are the most commonly used tool to perpetuate cyber violence against women, especially in emerging regions like Africa.

Viral rape videos, which have become particularly commonplace in South Africa, is one such example. There are also growing concerns over the use of technology to 'cyber stalk' victims. Increases in the availability of information online, for example through location tagging, may facilitate these forms of victimization and increase risks for victims. Even though South Africa has strict laws governing these types of behaviours, these are rarely enforced. Technology also has the potential to facilitate the prosecution of crimes in cases of gender-based violence.

While the Internet is a potential engine of equality, it has also often reinforced the power imbalances of offline realities; escalating cyber VAWG is one indicator that further cements and magnifies unequal power relations between men and women. Responding to this development are organizations like the Association for Progressive Communications (APC) which is both at the forefront of sounding the alarm about cyber VAWG and contributes to a global perspective to the discourse with the objective of reversing the tide against this form of violence against women and girls. APC and like-minded organizations are promoting anti-violent behaviours while acknowledging that technology, if properly instrumentalized can also be serve as an effective tool to combat all forms of VAWG.

4

TACKLING CYBER VAWG: A MULTI-LEVEL APPROACH

4.1 Pursuing a multi-level approach

The diagram below submits that most policy and practice fall into one of three categories of action:

1. Preventive measures through public sensitization and consciousness-raising;
2. Promotion of safeguards for safety and equality on the Internet for women and girls;
3. Putting in place and enforcement of sanctions.

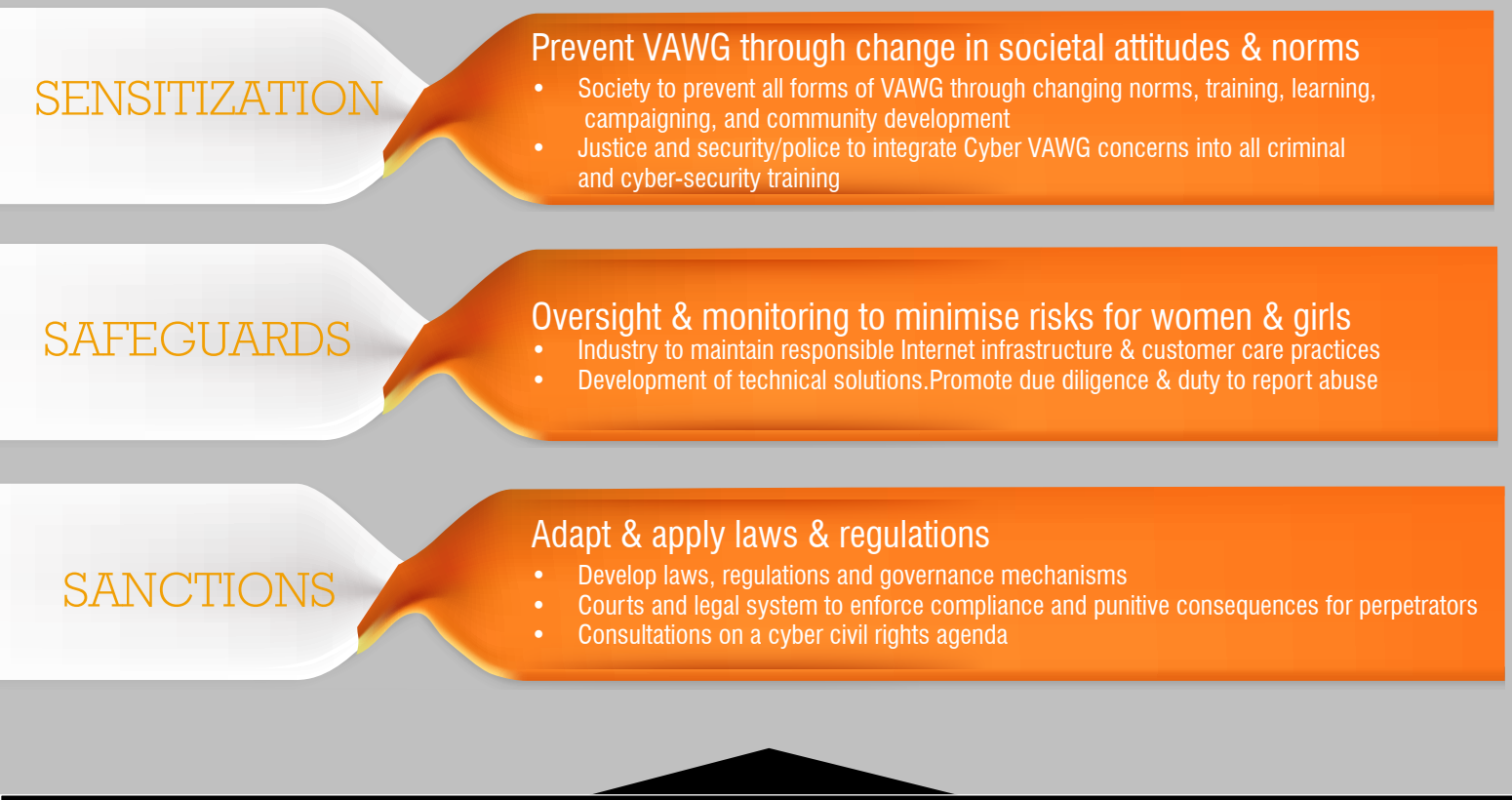
Each one of these pillars supports the others, and will need consistent, collaborative action at multiple levels.

4.2 Sensitization: changing societal norms

Article 5 of the CEDAW declares that States have an obligation to "take all appropriate measures to modify the social and cultural patterns of conduct of men and women, with a view to achieving the elimination of prejudices and customary and all other practices which are based on the idea of the inferiority or the superiority of either of the sexes or on stereotyped roles for men and women".

> "Anticipate problems and help solve them not only for yourself but for everybody else in the community. Act like a citizen. Not a passive 'user.' "
>
> *Rebecca MacKinnon, co-founder, Global Voice*

This language is critically important, and its operationalization truly impactful in terms of changing behaviours. The UN Human Rights Council agrees when it emphasized that "The prevention approach is the more sustainable [approach], focusing on change, whereas the State obligation to protect and punish remains relevant in combating violations".



Networked Intelligence for Development 2015

Sensitization includes:

- Bringing visibility and positive public consciousness to the issues to ensure that cyber VAWG online is neither ignored nor trivialized
- Sensitizing the next generation of ICT users; boys and girls; through their parents, teachers and wider communities including police and the justice system
- Breaking down communication barriers and outdated orthodox philosophies in learning environments.

4.2.1 Working towards a broad cultural base of change

Changing social attitudes and social norms is the first step to shifting the way online abuse is understood and the seriousness given to it. The public is in general ignorant about cyber VAWG and therefore less likely to consider it an issue of any consequence.

Given how ubiquitous technology has become, there is a need to acknowledge the evolution of the digital citizen (sometimes referred to as netizen). This includes media and information literacy, understanding of gender norms, digital footprints, security awareness, and more. There is a need to address social and cultural norms around gender and to bring these efforts into the digital age. In some countries, this can begin in the classroom through the education system, however, in many more countries, this is not an option. Other initiatives have sought opportunities to engage around these issues through youth as the next generation of internet users, building networks and alliances, and changing awareness and the content online through informal digital literacy programmes.

In particular there is a strong need to focus on violence prevention and community mobilization for zero tolerance for violence against women. Violence prevention works. Research shows that high school violence prevention programs that work with both boys and girls are highly effective over the long term. Similar to the anti-bully movement in schools, the cyberbullying movement

> "Culture is the sphere where we socialize ourselves, and the Internet – global in its reach – is a dimension of that sphere."
>
> *Jeremy Rifkin* [6]

has been gaining ground and impact. Positive changes in behaviour have led to awareness and new socialization. There is an opportunity to use this avenue to integrate cyber VAWG sensitization and prevention.

Examples of such initiatives include:

Tackling Violence Against Women Offline

- The Canadian Women's Foundation notes that: "Even years after attending one of our programs, students experienced long-term benefits such as better dating relationships, the ability to recognize and leave an unhealthy relationship, and increased self-confidence, assertiveness, and leadership".[62] Strong advocacy campaigns are vital to change — workplace harassment and drinking and driving are not acceptable behaviour and subject to serious criminal penalties. In the same way, public education, violence prevention programs, and a strong criminal justice response can bring about an end to online violence against women in Canada[63]. This type of prevention can be translated seamlessly to online safety measures.
- UN Women and the World Association of Girl Guides and Scouts program: Voices against Violence provides girls, boys, young women, and young men with tools and expertise to understand the root causes of violence in their communities, to educate and involve their peers and communities to prevent such violence, and to learn about where to access support if they experience violence.[64]
- In Europe, sport has been used as a vehicle to engage youth and change entrenched attitudes on gender equality in a number of countries including Tajikistan, Georgia and Kyrgyzstan.
- In Latin America, youth-targeted initiatives such as 'El Valiente No Es Violencia', a joint communications campaign with MTV, has gained momentum to establish zero tolerance to violence against women.
- The United Nations Secretary-General's Campaign UNiTE to End Violence against Women has proclaimed the 25th of each month as 'Orange Day', a day to raise awareness and take action against violence against women and girls. Orange Day calls upon activists, governments and UN partners to mobilize people and highlight issues relevant to preventing and ending violence against women and girls, not only once a year, but monthly.[65]
- Moraba is a mobile phone-based game designed to educate South Africa's township youth on gender-based violence. Developed by The Afroes Foundation for the UNiTE Campaign and UN Women.
- HeforShe Campaign is a UN Women-initiated solidarity movement that seeks the engagement of men to work with women in achieving gender equality and to challenge traditional notions of both femininity and masculinity. In 2015, Twitter and Vodaphone signed up as Impact Partners.
- In Bangladesh, UNDP helped develop the first ever *comprehensive knowledge space* on the government's information portal dedicated to VAW, as well as youth, police and parliamentary engagement in VAW.
- In November 2012, the National Human Rights Commission began a *VAW awareness social media campaign* targeting youth. In Albania, UNDP launched in 2013 a toll free number for women to report domestic violence.
- *Partners for Prevention* (P4P) is a multi-country research study on men and violence supported by UNDP which included capacity development for practitioners and decision makers, and communication for social change including support to campaigns that target men for change.

- *'Applying Social Media Tools for the Prevention of Gender-based Violence: Lessons learned from social media communication campaigns to prevent gender-based violence in India, China and Viet Nam'* was launched and disseminated in 2013. This resource consolidates learning from the P4P initiative 'Engaging Young Men through Social Media for the Prevention of Violence against Women'.

Let's Talk Men 2.0 is a film series launched in India, Pakistan, Nepal and Sri Lanka with accompanying tools for discussion facilitators. The films are designed to be used for years to come as tools for exploring gender norms and men's violence, especially with young people.

Tackling Violence Against Women Online

- In India, the *Centre for Cyber Victim Counselling* develops educational cyber-awareness programs for schools, for parents and for community members such as the police force.
- *Women's Aid* in the UK has created a practical guide for victims of online abuse entitled: Digital stalking: a guide to technology risks for victims. "Just five rules for what you can do on the site: Don't spam; Don't ask for votes or engage in vote manipulation; Don't post personal information; No child pornography or sexually suggestive content featuring minors; Don't break the site or do anything that interferes with normal use of the site."
- *Heartmob* is a platform that provides real-time support to individuals experiencing online harassment - and gives bystanders concrete actions they can take to step in and save the day.[66]
- "Cyber Nirapotta Program' has built awareness among 2,839 female college students about cyber security by arranging seminars from May 2014 to August 2014. Bangladesh Telecommunication Regulatory Commission (BTRC) formed a committee with 11 members to prevent the cyber crime.
- Setting up or supporting peer-support networks (e.g. the CyberMentors project from BeatBullying, beatbullying.org) and the development of and education in technical solutions to control abusive behaviour is an appropriate role for industry. Research in New Zealand suggests that industry should consider not only technical solutions but should also monitor their effectiveness in resolving cyberbullying complaints[67]
- COST Action on cyberbullying: Cooperation in the field of Scientific and Technical Research (COST) is an international network started in October 2008 to tackle "Cyberbullying: coping with negative and enhancing positive uses of new technologies, in relationships in educational settings". Its purpose is to share expertise on cyberbullying in educational settings, and now includes 28 European countries, has links to Action Poster, books and publications and a Guideline booklet translated into Czech, German and Turkish for preventing cyber-bullying in the school environment.[68]
- "To make the invisible visible" is the goal of Take Back the Tech! Map it! End it!! The project calls upon women and girls to take control of technology by telling their stories and shaping the narrative. It also seeks to hold witnesses and bystanders accountable. Women and girls can go online and document crimes committed and realise their experiences are not an isolated nor acceptable incidents.[69]

A broadly-based effective attack on cyber VAWG also needs to aggressively address and attack "victim blaming". This destructive response needs to be addressed as a primary issue of concern through a

panoply of educational and learning tools. There is no situation in which a violent act should be accepted or condoned as a result of poor personal judgement and social behaviour ("she should not have been dressed that way/ consumed alcohol/ invited the act upon herself").

> "Young people are the brokers, traders and advisors of this new knowledge and their voice provides a bridge between what they know and understand, and what researchers need to know and understand to properly inform policy and practice."
>
> *'Cyberbullying Through the New Media: Findings from an International Network'*

- In May 2013, following a week-long campaign by Women, Action and the Media, the *Everyday Sexism Project* and the activist Soraya Chemaly demanded the removal of supposedly humorous content endorsing rape and domestic violence. Facebook responded to concerted protests over content promoting violence against women, but only after fifteen companies, including Nissan, threatened to pull their advertisements if Facebook did not remove profiles that glorified or trivialized violence against women.[70] The company in turn determined to update its policies on hate speech and increase accountability of content creators and train staff to be more responsive to complaints, marking a victory for women's rights activists. "We prohibit content deemed to be directly harmful, but allow content that is offensive or controversial. We define harmful content as anything organising real world violence, theft, or property destruction, or that directly inflicts emotional distress on a specific private individual (e.g., bullying)."[71]

Digital Literacy and Citizenship and Gender Relevant and Friendly Content

There are a growing number of initiatives that address digital literacy and citizenship, and to varying degrees cover topics such as online safety and information literacy. These include efforts from civil society like Telecentre.org and ITU which has reached 1 million women with a digital literacy course and Common Sense Media which designed curricula that teaches media literacy as well as digital safety and smarts. The UK initiative iRights provides detailed guidance on online safety, security, right to remove, right to digital literacy including the ability to critique technologies and understand how to negotiate social norms. The private sector has also taken important steps in raising awareness – such as the recent GSMA report on Accelerating Digital Literacy for Women – and training as with the Intel She Will Connect initiative which builds women's digital literacy and includes modules on digital safety and footprints. There is also a role that the

individual must play in self-regulating, not perpetuating negative gender norms and practices by sharing, watching and listening and by holding media and content providers to account. This is an underlying message of the UNESCO Global Alliance on Gender and Media. [72]

Part of the solution to changing online culture is through the creation of gender sensitive and friendly content. This requires moving beyond digital literacy efforts that teach girls and women how to (safely) consume content, and moves them to the position of content creators and active contributors to and shapers of the online world. Efforts such as Mozilla's web literacy clubs place an emphasis not just on privacy and digital citizenship but also on content creation, coding skills and creating meaningful impact on the web. Through a partnership with UN Women a greater emphasis will be placed on reaching girls and women. Global networks and platforms like empowerwomen.org and World Pulse also provide digital literacy skills but also actively work with women to contribute their voice and perspectives on the web, including through blogs and campaigns. More women-friendly content would drive women online according to Egyptian high-income women who did not use the Internet but called for "new websites only for women" or "dedicated to women," or women-only chatting. Somewhat in the same vein, a high-income, university educated Indian professional who does use the Internet wanted cybercafés that are open only to women.[73] Safe access matters too.

4.2.2 Sensitization of the law, courts and enforcement officers

Strategies, laws and policies must demand a concerted effort that includes education, awareness raising, and sensitization and community mobilization. They must also contribute to tackling discriminatory stereotypes and attitudes, and they must mandate the research and knowledge-building necessary to support policy development. However, having laws in place alone is not sufficient. In South Africa, for example, VAWG remains rampant, irrespective of human rights – focused laws such as the Domestic Violence Act No 116 of 1998 and Criminal Law (Sexual Offense and Related Matters) Act No 32 of 2007 framed to protect women against all forms of violence. [74]

To effectively combat cyber VAWG, personnel and officials working in the field must have the skills, capacity and sensitivity to apply the spirit and letter of the law in a fully comprehensive manner. This requires that, among others: [75]

- Appropriate resources be devoted towards equipment and technological education of personnel employed in public institutions, such as schools and police forces. Individuals, teachers, parents, police, prosecutors and judges need to educate themselves about the technology, the behaviour and the harm inflicted.
- Police forces should be trained, properly resourced and given the necessary powers to reach out to victims to ensure all forms of VAWG in varied settings are recognised, recorded and acted on expeditiously. Following exhaustive reporting on the failures of law enforcement at all levels to comprehend the emotional, professional, and financial toll of misogynistic online intimidation[76]. US journalist Amanda Hess concludes: "The Internet is a global network, but when you pick up the phone to report an online threat, whether you are in London or Palm Springs, you end up face-to-face with a cop who patrols a comparatively puny jurisdiction. And your cop will probably be a man: according to the U.S. Bureau of Justice Statistics, in 2008, only 6.5 percent of state police officers and 19 percent of FBI agents were women. And in many locales, police work is still a largely analog affair as 911 calls are immediately

routed to the local police force, the closest officer is dispatched to respond and he takes notes with pen and paper." [77]

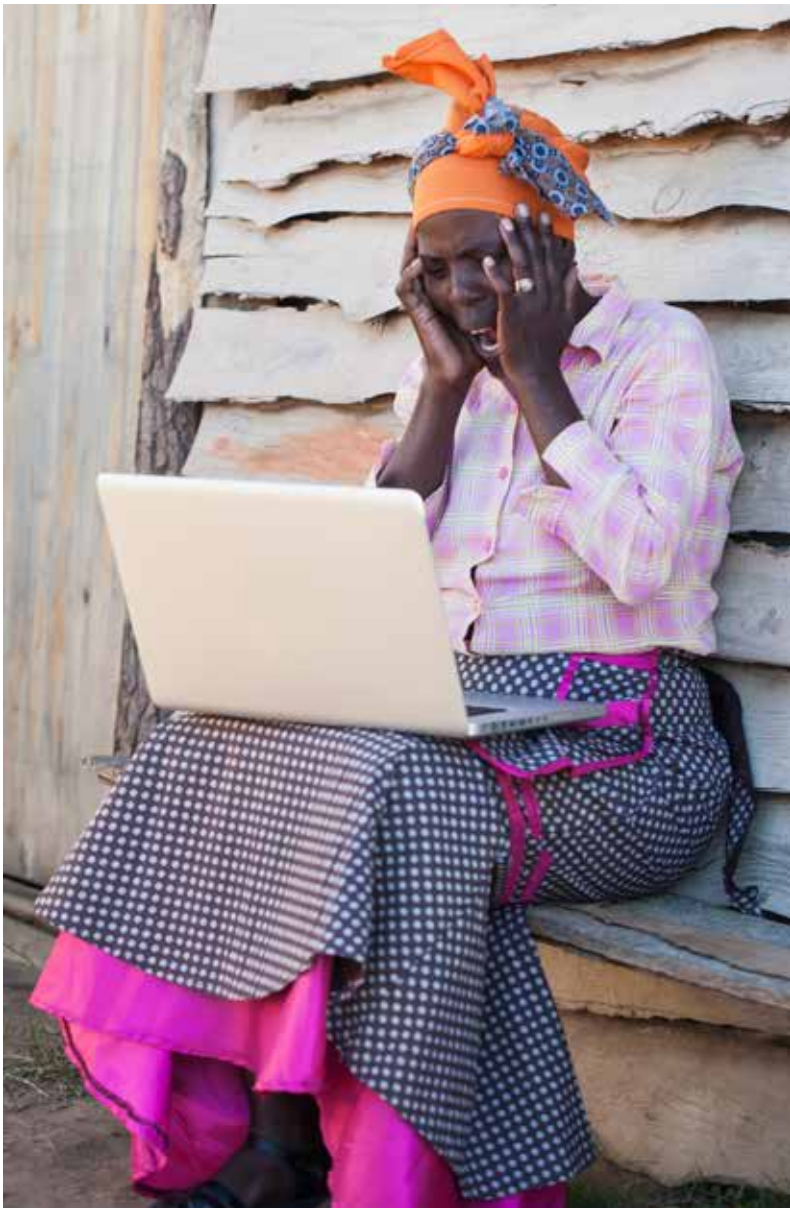
- Encouragingly, there are signs of positive developments in some countries. Dutch law enforcement is stepping up its efforts to combat cybercrime. Every regional police force in the country will train their detectives in digital investigative techniques. More ICT specialists and external experts will be recruited. Specialized digital detectives will join national and international investigative teams. A "national digital investigations action program" was established in July 2014, with a budget of EUR 1.4 million. Law enforcement however estimated that it needs EUR 30 million a year to effectively intensify the battle against cybercrime.

4.3 Safeguards: working with industry and users to make the Internet VAWG-safe

Over the years, traditional VAW safety measures have evolved to include women's shelters, crisis centres, help lines and education. In light of the new challenges in the dynamic ICT environment, the digital world also requires safety measures, and in order to keep up with a rapidly changing Internet, this will necessarily require resources, attention and active participation of industry, civil society and governments.

Free speech requires constant vigilance – by everyone who uses the Internet. What is the scope of safeguards needed to be integrated with Internet use?

Rima Athar and the APC team in their 2015 report[78] conclude that many Terms of Service (ToS) are more about legal obligations, and that "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 the safety of women is discussed, the focus is often on how women should be protected. But protection is not the same thing as security. The question should be what women need to safely participate in society.

Kvinna Till Kvinna Foundation

When we talk about safeguards, we must talk about legal liabilities that "are warranted and necessary to protect and respect women's rights."

4.3.1 Industry safeguard protocols

Industry players are important digital gatekeepers. They include ISPs, mobile phone companies (MPCs), hosts of social networking sites (SNS), online dating and gaming sites, and software developers. Website operators/ employers and investors are key sources of deterrence and remedy, and they should not be immune from social responsibility or from liability.

Companies need to explicitly recognise VAWG as unlawful behavior, and demonstrate increased and expedited cooperation in providing relief to victims/survivors within the capacities that companies have. In particular:

1. systems for cooperating with law enforcement;
2. takedown procedures for abusive and harmful content;
3. the possibility of account termination for misconduct;
4. production of transparency reports of records specific to VAWG, detailing how and when they have responded to them.

International human rights standards should be the guidelines. The Special Rapporteur on Freedom of Opinion and Expression, Frank La Rue, warns against filtering in his 2011 report: "The lack of transparency surrounding these measures also makes it difficult to ascertain whether blocking or filtering is really necessary for the purported aims put forward by States."[79]

"Each platform on the Internet needs to have a policy that clearly defines what they consider offensive and inappropriate. Users need to 'tick' their consent to respect at all times these polities and accept liability for violating them. Current policing of content on social media however does not support women against acts of cyber VAWG, nor do they represent a commitment to ending violence against women" [80] The Internet industry has been responding in a variety of ways to public demand for better monitoring and resolving of user complaints:

- In its community guidelines, *YouTube* advises users to 'use YouTube without fear of being subjected to malicious harassment. In cases where harassment crosses the line into a malicious attack, it can be reported and removed. Providing users with examples of speech that violates community guidelines would help foster learning and dialogue, and would better frame the concrete implications for certain misbehaviours.[81] The YouTube approach is generally regarded as an example of good practice, for it allows companies to educate their users without sacrificing their flexibility to address harassing speech.
- In April 2015, in an attempt to crackdown on abusive message, *Twitter* announced a new filter that would prevent users from seeing threatening messages. It also introduced temporary suspensions for accounts that fall foul of its policies.[82]
- *WhatsApp* excuses itself from monitoring of contents or messages by putting the burden of safe practices on the users and directing the victims to report the matters through takedown reports or self-protection mechanisms. Harassers or perpetrators take huge advantage of this situation since the level of awareness regarding safe practices in the WhatsApp is low in countries like India.[83]
- *Facebook* also puts the burden of safe practices onto the users, and while it routinely upgrades security settings, the guidelines are fairly opaque and not easily understood by the average users. ConsumerReports.org reported that 11 per cent

of households using Facebook in the US identified safety issues last year, ranging from someone using their log-in without permission to being harassed or threatened. This increase translates into 7 million affected households— a 30 per cent increase over the previous year.[84]

- In addition, 5.6 million underage kids have Facebook accounts and 800,000 minors reported to have been harassed or subjected to other forms of cyberbullying on Facebook.[85]Facebook currently bans users under 13 from joining the social network.
- In one case in September 2012, a California lawyer had his Facebook account hacked. The perpetrator inserted pornographic language into the fake profile and sent vulgar sexual messages daily to the man's friends, family, and business colleagues. It took more than a month to resolve the issues. In contrast, when private photos of Mark Zuckerberg were posted to Imgur, a photo-sharing site – the flaw was fixed in a day.

The Internet/cyber industry can also sign up to a code of practice framed within Corporate Social Responsibility. In a survey of the UK's ten leading ISPs, seven had posted CSR reports and policies on their websites with the majority of these focusing on sage and responsible use.[86]

The UK's *2008 Byron Review* advocates for an industry role in making the Internet a safer place for children stating: "We need a shared culture of responsibility with families, industry, government and others in the public and third sectors all playing their part to reduce the availability of potential harmful material, restrict access to it by children and to increase children's resilience."

Highlights on Internet intermediary liability: 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 in these three jurisdictions 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.[87] The Manila Principles on Intermediary Liability, while not VAWG specific, provide useful information and research.

Terms of Use in practice: There is no one-size-fits-all solution for the complex set of challenges raised by Terms of Use (ToU) enforcement. Platforms vary in terms of history, mission, content hosted, size, and user base, and no single set of practices will be an appropriate fit in every case. Moreover, while the examples in this report focus on platforms that host social media, the recommendations are broadly applicable to companies that host different types of user-generated content. They should acknowledge that companies can have a significant impact on user rights and user satisfaction by being clearer and more consistent in how they implement ToU and interact with users. And they are mindful that costs associated with creating channels for customer support, responses to user inquiries, appeals processes, and similar mechanisms should not be underestimated. Positive outcomes often rely on proactive and transparent communications with users from the outset and at each stage of interaction between the company and a user. It is in this context that recommendations cover primarily the following areas: Offer clear, consistent, and transparent ToU and guidelines:

- Respond when a suspected violation of the ToU is identified
- Provide opportunities for recourse: appeals, due Process, and data export
- Embed human rights considerations into company practice and platform design
- Recommendations for users.

Useful resources exist to help platforms design programs and policies that are consonant with human rights norms and practices. These include the *Global Network Initiative's Principles on Free Expression* and Privacy; the *Protect, Respect, and Remedy framework* created by John Ruggie, the United Nations Special Representative of the Secretary General on transnational corporations and other business enterprises; and the OECD's *Guidelines for Multinational Enterprises—Recommendations for Responsible Business Conduct in a Global Context.*[88] APC has also created a checklist for social media platforms based on the Ruggie framework titled: *Ensuring compliance with the UN Guiding Principles: A checklist for addressing violence against women.*

An interesting example of a "soft tool" used by government to discourage violence against women through ICTs is being proposed by the Government of Sweden in the form of a "seal" that will indicate whether video games are gender friendly.[89]

4.3.2 On-line safety tools and apps

To date there are a few security tools for women[90] that comprise innovative tracking, monitoring and reporting methods; they represent civil society's immediate response to dealing with VAWG. There has been a wave of safety technology developed for smartphone users: whistles to get bystanders' attention, GPS trackers to lead people to your location, automatic video recordings to capture proof of a crime, to name a few. For example, bsafe and guardly are free downloadable apps. Other examples include:

- HARASSmap is a mobile online technology that uses interactive mapping to try to reduce the social acceptability of sexual harassment throughout Egypt by monitoring harassment. Reports are mapped and appear as a red dot.
- SafetiPin is a map-based mobile personal safety

app. An individual user can conduct a safety audit, pin places where they feel unsafe or have faced any form of harassment. The app user is also able to see all the information that has been uploaded by others and make informed decisions about moving around the city safely. Women and men can see the Safety Score of any place in the city and can also use it when they visit new cities. The underlying belief is that if spaces are made safe for women, they will be safer for everyone.[91] In Rio de Janeiro, communities are identifying safety risks in 10 of the cities' high-risk slums (favelas). Trained women and adolescent girls use their smartphones to map safety risks such as faulty infrastructure or services, obscured walking routes, and lack of lighting. These initial findings were routinely presented to local authorities, and are being used to develop solutions.

- UN Women partnered with Microsoft to identify existing and potential use of mobile technologies for women's safety in public places. A global assessment and city reports from Marrakesh, Delhi and Rio are available.
- The *National Human Trafficking Resource Center* (Polaris Project) helped to launch BEFREE text shortcode, an SMS-based hotline integrated into the National Human Trafficking Resource Center. Available 24 hours a day, seven days a week, the text allows victims to anonymously and discretely reach out for help. Organizations from around the world such as La Strada International, and Liberty Asia also have hotlines that trafficking victims can call for assistance. Not only do these hotlines provide victims with a support system that can assist them in getting out of danger, they also provide useful data on trafficking operations themselves.
- Call blocking apps are also growing in use. GSMA notes "one of the biggest trends in emerging

WOMEN IN TECH

16 (global)
40 (within regions) %

Gender Access Gap to internet and mobile phones. Multiple studies in all regions from the last two years also show a significant gender gap in sophistication of use of technology which is growing and harder to close. (BC Gender Working Group, Intel, GSMA, ITU)

10-15%

of high levels managers in technology are women (*ITU*)

11%

of game designers (an industry in the billions and with great reach) are women (3% are actual programmers) (*BostonGlobe*)

10%

is the cap of women in innovation tech hubs in every region in the world (but Bangalore at 20%) (*GSMA, Telefoncia 2012*)

9%

of apps in Europe are created by women (*EC*)

7%

of VC funded start-ups are led by women (*MIT*)

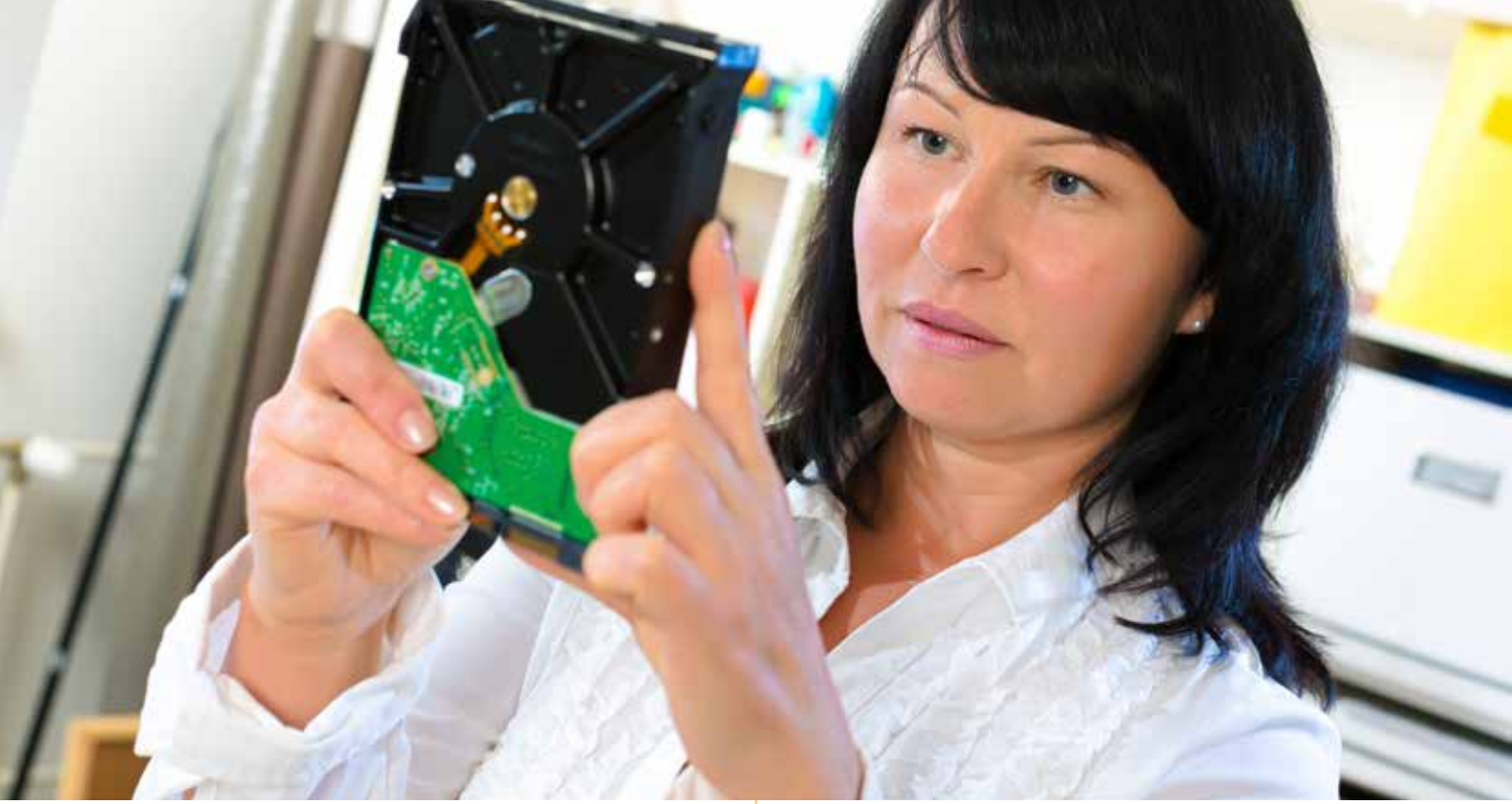
6%

of ICT regulators and Ministers (the figure is dropping) and of CEOs of top 100 tech firms are women (*ITU*)

1%

women at the Consumer Electronics Show felt that products were created with them in mind (*4b.com*)

Source: UN Women, ICT and Gender Equality: In Brief



market app stores – the explosion in popularity of call blocking apps. These apps allow mobile users to identify and block harassing mobile numbers and often include features that can reveal the name or location of the caller. One of the most popular call blocking apps is Truecaller, an app which last year saw 500% growth among sub-Saharan African users. Today Truecaller has over 100 million users worldwide, hardly an insignificant figure when compared with app giants Instagram (~300m users), Twitter (~240m users) and Snapchat (~200m users).[92]

4.3.3 Women in the Tech Sector

Finally, the lack of women in the technology sector – including in private and public sector - may also have an impact on priorities, culture, technologies developed and corporate policies, regulations and infrastructures that can promote or reduce cyber VAW. Technology tends to reflect the interests, perspectives and experiences of those creating them. The discrepancy between the need to address cyber VAW and the present gaps in attention to developing solutions may not be surprising then when looking at the figures of women in technology, particularly in decision making positions.

A concerted effort to promote more women into decision-making positions in the technology sector should be a high priority. Moreover, there is a need to engage men within the tech sector as well. The Cisco Men for Inclusion programme is one such example and may serve as a reference for other companies.[93]

4.4 Sanctions and compliance: Frameworks, Law and its application

No matter the platform employed, growing cyber-crime calls for an explicit incorporation of the relevant and human rights conventions and constitutional laws into Internet governance. The UN system - and importantly the ITU and UN Women as respective leads on ICT regulations and EVAW - is in a unique position to bring industry together with governments to bring about much needed clarity and provide the necessary incentives, resources and political will to champion and address cyber VAWG. In addition, the global community has through normative frameworks has established commitments that either explicitly or implicitly require governments and other stakeholders to take action.

4.4.1 Global Rights and Normative Frameworks

In addition to previously mentioned rights frameworks and conclusions from the Special Rapporteur on Freedom of Expression the following provide guidance and commitments for action:

- Post2015 Agenda - Sustainable Development Goals: The Sustainable Development Goals stand-alone goal to achieve gender equality tackles structural causes by highlighting three critical areas that are holding women back. The first area is violence against women. Moreover, it also includes women's use of enabling technology, including ICTs, as a means of implementation of the gender goal.
- Section J of the *Beijing Platform for Action* — on women and the media — needs to be reprioritised in the context of the post-2015 development agenda. Advocacy for the reprioritisation of Section J at the CSW asked governments to recognise the critical role that the media and information and communications technologies (ICTs) play in both advancing and stifling women's rights. The Secretary General Report included a detailed assessment of progress and gaps and number of priority forward looking recommendations. APC has also developed 10 points on Section J which describes the growing impact of ICTs on a variety of women's rights issues – from access and agency to economics and ecology.[94]
- Commission on the Status of Women: The 2013 CSW outcomes recommended that States should: "Support the development and use of ICT and social media as a resource for the empowerment of women and girls, including access to information on the prevention of and response to violence against women and girls; and develop mechanisms to combat the use of ICT and social media to perpetrate violence against women and girls, including the criminal misuse of ICT for sexual harassment, sexual exploitation, child pornography and trafficking in women and girls, and emerging forms of violence such as cyber stalking, cyber bullying and privacy violations that compromise women's and girls' safety."
- Convention on the Elimination of the Discrimination Against Women (CEDAW): As with other rights frameworks CEDAW should be interpreted through a 21st century lens by considering online violence against women within national reporting or through general comments.
- In the context of cybercrime, stakeholders, including the UN system have noted the need to balance rights. Groups such as APC have cautioned that in the name of spurious measures to "protect" women online we need to be weary of censorship, and that efforts should strive to "balance rights to privacy, freedom of expression and freedom from violence and harassment for all individuals in constitutional, civil and criminal law."[95]

4.4.2 National Laws and Regulations

While laws, regulatory frameworks and civil society action on all aspects of VAWG at national levels are all extremely important, overarching safeguard standards, policy guidance and accountability needs Internet industry leadership as well.

In 74% of Web Index countries, the Web Foundation found that law enforcement agencies and the courts are failing to take appropriate actions for cyber VAWG.[96] Furthermore, one in five female Internet users live in countries where harassment and abuse of women online is extremely unlikely to be punished.[97] Locally relevant information on sexual and reproductive health rights and services and gender-based violence is available via phone or browser in only 37% of countries.

The emerging *Internet of Things* will connect every machine, business, residence and vehicle in an intelligent infrastructure of communications, services and logistics. Estimates suggest that by 2030 100 trillion sensors and pFiD chips will be embedded in day-to-day gadgets and applications. Cyber-crime experts indicate that this may have serious implications for the harassment and tracking potential of cyber VAWG. When such a high proportion of human and object is connected, what boundaries or firewalls need to be established to protect an individual's right to privacy and safety, and to provide recourse if these boundaries are tampered with? What governance and legal frameworks that enable the right to access as well as the right to withdraw need to be put in place and enforced? And who oversees the virtual public space?

The international community under the leadership of the United Nations system needs to find ways to build Internet protocols and regulations to assure transparency, objectivity and the identification of illegal activities, including cyber VAWG. When the interconnectivity, instantaneity and insulation of the Internet and social media is used to facilitate campaigns of harassment, intimidation, humiliation, emotional distress and terror against targeted individuals"[98] how should we, as citizens, consumers and as women, respond?

Laws have an important role to play; they complement regulatory protocols targeting website operators and employers – who are important players in deterrence and remedy. However, a legal reform agenda must be broad based to maximize reach and impact. There is a mix of legal frameworks that could effectively respond to cyber-crime and cyber VAWG. It includes, among others:

1. Information and communication laws (e.g. laws concerning Internet regulation or Internet content and intermediary services)
2. Data protection/privacy law99
3. Constitutional laws and human rights law (e.g. laws concerning freedom of expression/speech)
4. Criminal laws (e.g. laws concerning violence against persons; terrorism; prostitution, cyberbullying)

- Traditional legislative frameworks are historically territory-specific, whereas SNSs are global in nature and reach. What needs to be solved are persistent difficulties in effective cooperation and law enforcement across geographical borders and legal jurisdictions. For example an SNS could be in a different legal jurisdiction to the user, and this may not be able to ascertain the ISP identity, nor may it always be able to trace the perpetrator and ban them from the site. While complicated to pursue, this is not an excuse for them not to manage cyber-violence risks.

- Uncertainty about who the attackers 'really' are in a world of fluid identities, fears about heightened attacks, a lack of awareness – or a mistrust – of legal systems; all serve as potential barriers to addressing what is a growing problem for women across the world.[100]
- Add to this mix of difficulties a diversity of legal definitions. Cyber-bullying for instance may not be considered illegal throughout jurisdictions and therefore is not subject to laws around removal of illegal content.

In an effort to modernize its defamation law, the UK Parliament recently enacted the *Defamation Act* 2013, of which Section 5 sets up a "notice-and-takedown" system for defamation from user-generated content (UGC). If the website operator cannot provide authenticated identifying information about its users, the website operator will lose the act's protection.

The United States does have a notice-and-takedown scheme for copyright infringing UGC but the safe harbor

does not require websites to authenticate users or attribute their content. Websites must turn over information about their users on request, but they aren't required to collect or keep information about their users. Otherwise, websites generally aren't liable for UGC, whether or not potential plaintiffs can find the users to sue.

In Malaysia, the owner and operator of one of the largest Wi-Fi networks in the country, stressed that issues such as tracking who is responsible for putting up malicious, defamatory and seditious comments in cyberspace is essentially a technological issue, and as such, must be addressed in a technical way.

Bytes for All (B4A) in Pakistan is a human rights organization and a research think tank with a focus on ICTs. It experiments with and organizes debates on the relevance of ICTs for sustainable development and the strengthening of human rights movements in the country, with emphasis on gender.

4.4.3 Applying the language of laws against violence against women to cyber VAWG

In practice, taking a legal approach is often the last resort for women and is usually available to those with financial resources and empowered with knowledge through education. Most VAWG offences go by unreported. A 2014 APC report maps cyber VAW experiences across seven countries (Pakistan, Colombia, Mexico, Bosnia-Herzegovina, DRC, Kenya & Philippines) and their attempts to access justice either through domestic legal remedy or corporate grievance mechanisms.

> *"In each country we witness various forms of cyber violence, and it is evident that the real threat to women and girls is the double tragedy of lack of agency and resources victims have in dealing with the offences committed against them" 2014 APC Report* [101]

The report delved into the adequacy and effectiveness of laws, the culture of impunity, and survivors' own agency and power. APC concluded that "…even though the women interviewed came from a range of socioeconomic backgrounds and diverse geographical locations, they

were all aware that a crime had been committed against them and that they were entitled to some form of redress. Ultimately it remains the duty of the state to uphold women's rights."[102]

The APC report also found that women's access to justice was negated by:

- The complexities in the law itself;
- The structural or systemic failure of the law to address technology-related VAW and to respond to women seeking access to remedies in cases of violence;
- The prevailing attitudes in society and of the duty bearers characterised by gender bias and discrimination;
- A culture of impunity whereby the legal system was perceived as unable to address VAW, and the assumption that perpetrators would not be punished.

Nonetheless, some examples of emerging laws include the following:

- In the Unites States, Congress passed the *Violence against Women Act* in 1994 (VAWGA 1994) as part of the Violent Crime Control and Law Enforcement Act of 1994. The protections and provisions afforded by the 1994 legislation were subsequently expanded and improved in the Violence Against Women Act of 2000 (VAWGA 2000) and the Violence Against Women and Department of Justice Reauthorization Act of 2005 (VAWGA 2005).[103]
- In 2014, six states in the USA have criminalised revenge porn - Alaska, California, Idaho, Maryland, New Jersey and Utah[104]. Revenge porn bills are pending in twenty two states. The terms have to be specifically defined to clarify what is meant by the term 'sexually explicit'. A model state law is suggested by Citron.[105]
- Canada: *Investigation and Preventing Criminal Electronic Communications Act* (2012) (Bill C-30) place greater restrictions and reduce privacy online by requiring ISPs to retain data for longer periods of time (thus making them available by subpoena without individual notification). The Government of Canada has introduced Bill C-13, the *Protecting Canadians from Online Crime Act*, which would make it a criminal offence to distribute intimate images without the consent of the person depicted.
- India: *Indecent Representation of Women (Prohibition) Act* 1986 (IRWA), is currently under consideration for amendment by Parliament to include virtual spaces.[106] Indian laws regarding

data privacy, offensive communication through Internet and digital communication technology and jurisdictional issues in cases of crimes committed through ICT and DCT still need to be developed.[107]

- Estonia: digital privacy clauses for pre-nuptial and post-nuptial agreements have been adopted so that spouses cannot use texts, emails or photos against each other in case of divorce.
- Others have suggested the establishment of a *Cyber Civil Rights Initiative* (CCRI) at local and national levels as described by Citron is indispensable.[108]

4.4.4 Other Approaches: National Strategies

In addition to the development and application of national laws and more effective global governance regimes, there are other incentives that can be put in place at the national level through ICT and EVAW related strategies. The Policy Work stream of the Broadband Commission Gender Working Group in its 2014 background paper[109] noted a number of approaches that can successfully address VAW directly as well as address underlying ecosystem issues.

- In Spain, under their strategy for gender inclusion in the information society, financial incentives were given: to companies that developed web spaces which made visible the contributions of women to all fields of knowledge; for incorporation of ICT in the associations of women; and for software development that promote non-sexist values (e.g. games).
- In Mexico's Digital strategy, there is a focus on the development of several government supported platforms that support the inclusion of women, for example: entrepreneurs and business owners, life without violence, local development portal for gender equality, gender in the spotlight, spaces for gender advocates in civil society, gender indicators, opportunities for appropriation of ICT and digital skill development, educational content and online learning aimed at girls and teens, and programmes aimed at preventing violence through ICT. Under this strategy, an important link is the coordination between the National Institute for Women (National Institute for Women) and the digital agenda.

In addition, the Alliance for the Affordable Internet has been active in ensuring that women's organizations and gender advocates are active participants in the development of national Broadband Strategies. In countries such as Nigeria, Ghana, and the Dominican Republic, gender advocates have been instrumental in defining policy agendas and implementation plans. This is essential for legitimacy and responsiveness of national strategies to women's needs and gender equality issues.

APC has been doing the same in brining ICT issues to the attention of gender advocates through its Feminist Tech Exchanges (FTX) which provide skills diffusion and capacity building to empower women's rights organisations, advocates and feminists sidelined in the growth of the global digital commons. The Exchange has been developed in response to the expressed needs of feminist and women's rights movements for greater understanding of emerging ICT and applications.[110]

However, there are still significant gaps on both sides of strategies, as well as a need to bridge these — technology and gender equality — communities.

5

A VIEW TO ENDING CYBER VAWG THROUGH PARTNERSHIPS AND COALITIONS

Working with platforms that provide for and enable meaningful participation in policy discussion and decision making by and for women will be an important step to build a strong foundation. Global multi-stakeholder processes can also provide collaborative space to discuss complexities in policies and legal debates that surround cyber VAWG, such as questions of balancing safety of women from violence on the one hand and freedom of expression on the other hand, or question of Internet intermediaries liability.[111]

The majority of big and small Internet companies can be expected to support a system of checks and balances; that the power for investigations into harassment, threats of physical safety, sexual violence, kidnapping (etc.) must ultimately lie with courts and law enforcement; and that therefore laws that direct companies in their responsibilities are necessary. However, the waters start to muddy when it comes to compliance and prosecuting.[112] Some examples include:

- The *Inter-parliamentary Task Force on Internet Hate* passed a formal resolution establishing the Anti-Cyber-hate Working group made up of industry representatives, nongovernmental organisations, academics and others to 'build best practices for understanding, reporting upon and responding to Internet hate"
- The world's largest regional security organization, the *Organization for Security and Co-operation in Europe* (OSCE) promotes comprehensive security through conflict prevention, crisis management and post-conflict rehabilitation. The OSCE addresses VAW as a serious obstacle to the realization of gender equality. The persistence of

violence against women represents a significant security challenge for all OSCE participating States, and addressing this challenge is at the heart of the OSCE mandate.

- The *Internet Governance Forum* (IGF) can play an important role in addressing cyber VAWG, given its holistic approach and engagement of variety of actors – states, women's rights organizations, Internet intermediaries and users. The IGF is bringing together multiple stakeholders to outline what constitutes abuse of women, factors that contribute to enabling environments for abuse and the impacts that such abuse has in communities. Solutions and strategies resulting in best practices are also being addressed. The Best Practices Forum (BPF) is working to produce a tangible output for IGF 2015 on the question: *What are effective practices and policies that address, mitigate and/or prevent the abuse of women online?* Through organized fortnightly calls and using an inclusive, transparent and iterative multi-stage process, the BPF aims to gather input from multiple stakeholders. [113]

> "...states have an obligation to exercise due diligence to prevent, investigate and punish acts of violence, whether those acts are perpetrated by the state or private persons, and provide protection to victims..."
>
> *(Recommendation (2002) 5 of the Committee of Ministers of the Council of Europe to member states on the protection of women against violence).*

The UN System has also been examining engagement around cyber security issues from different perspectives, including rights frameworks, and developing a system wide plan on how to address cyber security and crime.[114] UNODC has been working at the forefront of cybersecurity and has noted that threats to Internet safety have spiked dramatically in recent years, and cybercrime now affects more than 431 million adult victims globally and that the Internet has become a breeding ground for criminal activity related to child pornography and abuse material.[115] It has been delivering technical assistance to law enforcement authorities, prosecutors, and the judiciary, in three regions of the world, in Eastern Africa, South-East Asia, and Central America. Because developing countries lack the capacity to combat cyberattacks and other forms of cybercrime, criminals will exploit countries' legal loopholes and weak security measures to perpetrate cybercrimes.

Other examples of emergent thinking come in the form of the *Feminist Principles of the Internet* provide an innovative, holistic and inclusive framework that speaks to the intersections of gender and sexuality with Internet freedoms.[116] The principles are being shared with Internet governance bodies in Bosnia and Herzegovina, India, Indonesia and the DRC, among other countries. There is a coalition advocating for these principals and related commitments, including within WSIS, CSW, IGF and the SDGs.

6

CONCLUSIONS AND PRINCIPLES FOR FURTHER ACTION

We are faced with two priorities that require immediate attention: eliminating cyber abuse and violence against women and reproduction online of offline harmful gender based practices; and the use of technology to combat multiple forms of violence against women and as vehicles for systemic change. As this framework suggests, the solutions are multi-dimensional in nature. In sum, the following considerations underpin and guide further action:

- Solutions can be found in innovative ICT technologies, the media and gaming industry, content creators and disseminators, users of the Internet, policy makers, and the regulators in the absence of 'the industry' able and/or willing to self-regulate. Efforts to ensure that governance structures, strategies, investments, the tech sector (public and private), access, and skill development are inclusive and gender responsive are requisites.
- Solutions can also be found through a mix of programs, projects and laws that bring about increased sensitivity toward the need to change social norms and behaviours. Included in this mix are 'hard' safeguards as defined and implemented by stakeholders to brace/support/facilitate an Internet that is VAWG-safe. Should this mix still not bring about the needed change, sanctions and enforced compliance with newly crafted regulations, laws and conventions will be necessary.

Online diligence, monitoring and reporting against violence and related crimes is everyone's business but responsible leadership roles must be played by:

- Telecoms and search engines, the indispensable backbone bringing the content to users, have a particular role and responsibility to protect the

public from violent or abusive behaviours

- Political and governmental bodies need to use their licensing prerogative to ensure that only those Telecoms and search engines are allowed to connect with the public that supervise content and its dissemination
- Regulators have a role to play,even if the solution to this challenge must be sought primarily in political realm
- Collaboration among media and technology unions, associations, clubs, organizations, professionals and women's media networks is also critical to promote women's leadership and decision-making in media and such technologies.[117]

Part of the 'soft' mix is the growing movement around *digital citizenship,* which represents an evolution in our norms — the ways we think about our personal responsibility, and the ways we respect and look out for others online. Studies have shown that the more removed you are from a situation; the less likely you are to act. Now that a cyber-touch is recognized as equally as harmful as a physical touch, all citizens, must prepare themselves to take the appropriate action. Responsibility begins with individual users, and extends to all participants in the online ecosystem — the users, publishers, providers and developers that define our common digital worlds.

Ultimately, this is also a *people-centred challenge* and one that must be tackled hand in hand with broader efforts around ending violence against women and gender equality:

- A broad based movement. Care needs to be taken not to stereotype or place disproportionate importance on one form of violence over another. Instead, the response to online offences against girls and women should be seen as part of the broader movement against sexual exploitation and abuse of any kind.
- Core roots of mainstreaming violence. There is widespread representation of VAWG in mainstream culture, including in contemporary and popular music, movies, the gaming industry and the general portrayal of women in popular media. Recent research on how violent video games are turning children, mostly boys, into 'killing zombies'[118] are also a part of mainstreaming violence. And while the presentation and analysis of this research is beyond the scope of this paper[119], the links to the core roots of the problem are very much in evidence and cannot be overlooked.
- Keeping up with the pace of change. The challenge of keeping up with the technological pace of change will require a parallel pace of change in the social behaviours and norms of netizens. An 'open-source' approach to changing behaviours is needed with the help of an enlightened networked society.
- Social movement using ICTs. When social movements successfully condemn and delegitimize a social practice, judges and politicians often jump on the bandwagon. The same technologies that allow citizen rights to challenge authoritarian governments also allow for public alarm over online sexual crimes. On the home and the workplace fronts, the women's movement has discredited the reasons behind society's protection of domestic violence and sexual harassment and engaged the attention of lawmakers, the courts and law enforcement.[120] This is an ongoing dialogue even in some countries where domestic laws against VAW are only just being enforced.

BIBLIOGRAPHY

- Afrihive (2014) African hubs at the forefront of catalyzing women in Technology, http://afrihive.com/african-hubs-at-the-forefront-of-catalyzing-women-in-technology/
- Association for Progressive Communications. (2014). "Feminist Principles of the Internet: An Evolving Document." Developed at the Gender, Sexuality, and Internet Meeting. 13-15 April, 2014. Malaysia. http://www.genderit.org/sites/default/upload/fpi_v3.pdf
- Association for Progressive Communications (2015) Cases on women's experiences of technology-related VAW and their access justice, https://www.apc.org/en/pubs/cases-women%E2%80%99s-experiences-technology-related-vaw-a
- Association for Progressive Communications (2015) 4 Reasons Women Fail to Access Justice in Tech-based VAW, http://www.genderit.org/sites/default/upload/csw_eng_web.pdf
- Athar, Rima. (2015). End violence: Women's rights and safety online. From impunity to justice: Improving corporate policies to end technology-related violence against women. Ed. Richa Kaul Padte. Published by Association for Progressive Communications (APC). March 2015. http://www.genderit.org/sites/default/upload/flow_corporate_policies_formatted_final.pdf
- BBC World Inc and GlobeScan. (2014). World Poll, EMBARGO 23:01 GMT 31 March 2014. Accessed 8 April 2015. http://www.globescan.com/images/images/pressreleases/2014-BBC-Freedom/BBC_GlobeScan_Freedom_Release_Final_March25.pdf
- BBC World Service Poll. (2010). Access to Internet As a Fundamental Right - study done by GlobeScan
- http://www.globescan.com/news_archives/bbc2010_Internet/index.html
- Boston Globe (2013), Women Remain Outsiders in Video Game Industry, https://www.bostonglobe.com/business/2013/01/27/women-remain-outsiders-video-game-industry/275JKqy3rFylT7TxgPmO3K/story.html

- Bridges, A., & Wosnitzer, R. (2007). Aggression and sexual behavior in best-selling pornography: A content analysis update. International Communication Association. (via http://stoppornculture.org/about/about-the-issue/facts-and-figures-2/)
- Broadband Commission Gender Working Group (2014) Draft Analysis: Gender and ICT Policy Workstream, www.empowerwomen.org/ict4d
- Broadband Commission Gender Working Group (2013) Doubling Digital Opportunities - enhancing the inclusion of women & girls in the Information Society, http://broadbandcommission.org/Documents/publications/bb-doubling-digital-2013.pdf
- Canadian Women's Foundation. "The Facts About Violence Against Women." Accessed 25 April 2015. http://www.canadianwomen.org/facts-about-violence
- Carter, Claire. "Twitter troll jailed for 'campaign of hatred' against Stella Creasy." *The Telegraph*, Accessed 29 September 2014. http://www.telegraph.co.uk/news/uknews/crime/11127808/Twitter-troll-jailed-for-campaign-of-hatred-against-Stella-Creasy.html
- Citron, Danielle Keats. (2009). "Law's expressive value in combating cyber gender harassment" Michigan Law Review, Vol. 108:373. 14 October 2009. http://digitalcommons.law.umaryland.edu/cgi/viewcontent.cgi?article=1687&context=fac_pubs
- Due Diligence Project. Accessed 12 May 2015. www.duediligenceproject.com
- European Union Agency for Fundamental Rights. (2014). Violence against women: an EU-wide survey Main results. Belgium. http://fra.europa.eu/sites/default/files/fra-2014-vaw-survey-main-results-apr14_en.pdf
- Facebook. (2015). Statement of Rights and Responsibilities. Date of Last Revision: 30 January 2015. Accessed 24 April 2015. https://www.facebook.com/legal/terms
- Fairbairn, Jordan, Dr. Rena Bivens and Dr. Myrna Dawson. (2013). Sexual Violence and Social Media: Building a Framework for Prevention. Ottawa, August 2013. http://www.octevaw-cocvff.ca/sites/all/files/pdf/reports/sexual-violence-and-social-media.pdf
- Fascendini, Flavia and Kate□ina Fialova (2011) Voices from Digital Spaces: Technology Related Violence Against Women, ed. Maia Marie (n.p.: Association for Progressive Communications, 2011), accessed April 25, 2014. http://www.apc.org/en/system/files/APCWNSP_MDG3advocacypaper_full_2011_EN_0.pdf
- Fulu, E., Warner, X., Miedema, S., Jewkes, R., Roselli, T. and Lang, J. (2013).
- Why Do Some Men Use Violence Against Women and How Can We Prevent It? Quantitative Findings from the United Nations Multi-country Study on Men and Violence in Asia and the Pacific Bangkok: UNDP, UNFPA, UN Women and UNV
- GenderiT.org. "Cases on women's experiences of technology-related VAW and their access to justice." 8 January 2015. Published by APC. Accessed 15 April 2015. http://www.genderit.org/node/4221
- GlobeScan. Accessed 7 April 2015. http://www.globescan.com/

- GlobeScan. (20). Water Aid Thought Leadership on Access to Water and Violence Against Women - study done by GlobeScan. Accessed 7 April 2015. http://www.globescan.com/component/edocman/?view=document&id=45&Itemid=0
- Goldstein, Phil. (2014). "Report: Global smartphone penetration to jump 25per cent in 2014, led by Asia-Pacific. " *Fierce Wireless*. 11 June 2014. Accessed 20 May 2015. http://www.fiercewireless.com/story/report-global-smartphone-penetration-jump-25-2014-led-asia-pacific/2014-06-11
- Griffen, Rachel. Is the Internet Safe Anymore? Website: Live Life Safe: Suzy Lamplugh Trust. Accessed 7 May 2015. http://www.suzylamplugh.org/2014/09/Internet-safe-women-anymore/
- Internet Live Stats. Accessed 24 April 2015. Available at: http://www.Internetlivestats.com/Internet-users/
- Halder, Debarati & K. Jaishankar (2015). Harassment via WHATsAPP in Urban & Rural India. A Baseline Survey Report (2015) file:///C:/Users/owner/Downloads/CCVCresearchreport2015.pdf
- Hess, Amanda. (2014). "Why Women Aren't Welcome on the Internet." Pacific Standard. 6 January 2014. Accessed 10 April 2015. http://www.psmag.com/health-and-behavior/women-arent-welcome-Internet-72170
- Intel Corporation and Dalberg Global Development Advisors. (2012). "Women and the Web:
- Bridging the Internet gap and creating new global opportunities in low and middle-income countries."
- http://www.intel.com/content/dam/www/public/us/en/documents/pdf/women-and-the-web.pdf
- Internet Governance Forum. Website. Accessed 14 April 2015. http://www.intgovforum.org/cms/best-practice-forums
- Kee, Jac sm. (2005). "Cultivating violence through technology? Exploring the connections between information communication technologies (ICT) and violence against women (VAW)." The Association for Progressive Communications. Available at: www.genderit.org/sites/default/upload/VAW_ICT_EN.pdf
- Kee, Jac sm and Sonia Randhawa. (2009). "Malaysia: Violence against Women and ICT" http://www.genderit.org/sites/default/upload/malaysia_APC_WNSP_MDG3_VAW_ICT_ctryrpt.pdf
- Knowledge Partnership Programme. (2014). Safetipin – An Overview Active Learning Solutions. http://www.ipekpp.com/admin/upload_files/Report_4_44_Safetipin_9496164970.pdf
- Kovacs, Anja, Richa Kaul Padte and Shobha SV. (2013). "Don't Let it Stand!"An Exploratory Study of Women and Verbal Online Abuse in India. Internet Democracy Project. New Delhi, India. April 2013. http://Internetdemocracy.in/wp-content/uploads/2013/12/Internet-Democracy-Project-Women-and-Online-Abuse.pdf
- Kvinna till Kvinna Foundation. (2012). "Women's security is ignored." Stockholm.
- http://kvinnatillkvinna.se/en/files/qbank/792c7b5aae4a79e78aaeda80516ae2ac.pdf
- Latonero, Mark. (2011). Human trafficking online: The role of social networking sites and online classifieds. USC Annenberg School for Communication and Journalism: Center on Communication Leadership & Policy Research Series. Available at: http://technologyandtrafficking.usc.edu
- Levy Paluck, E. & Ball, L. (2010). Social norms marketing aimed at gender based violence: A literature review and critical assessment. New York: International Rescue Committee.

- Messina, Lenlen. (2010). "Violence Against Women (VAW) in the Digital World: Emerging Issues, Challenges and Opportunities." ISIS International, No. 1, 2010 Women in Action. http://www.isiswomen.org/index.php?option=com_content&view=article&id=1475
- Newland, Erica and Caroline Nolan and Cynthia Wong and Jillian York. (2011). Account Deactivation and Content Removal: Guiding Principles and Practices for Companies and Users. The Berkman Center for Internet & Society and The Center for Democracy & Technology at Harvard University. 20 September 2011. http://cyber.law.harvard.edu/sites/cyber.law.harvard.edu/files/Final_Report_on_Account_Deactivation_and_Content_Removal.pdf
- Organization for Security and Co-operation in Europe. (2009). *"Bringing Security Home: Combating Violence Against Women in the OSCE Region." A Compilation of Good Practices"*. Ed. Jamila Seftaoui. Vienna, 2009.
- Viswanath, Kalpana and Ashish Basu. (2015). "SafetiPin: an innovative mobile app to collect data on women's safety in Indian cities. " *Gender & Development*, 2015. Vol.23, No.1, 45-60. Oxfam GB 2015. http://dx.doi.org/10.1080/13552074.2015.1013669
- Padte, Richa Kaul. (2013). "Keeping Women Safe? Gender, Online harassment and Indian Law." Internet Democracy Project. 29 June 2013. http://Internetdemocracy.in/reports/keeping-women-safe-gender-online-harassment-and-indian-law/
- Pew Research Center. (2014). "Online Harassment" 22 October 2014. Available at: http://www.pewInternet.org/2014/10/22/online-harassment/
- PEW Research Centre (2014). Online Harassment.
- West, Jessica. (2014). Cyber-Violence Against Women. Prepared for Battered Women Support Services, Vancouver, May 2014.
- http://www.bwss.org/wp-content/uploads/2014/05/CyberVAWReportJessicaWest.pdf
- Raja, Tasneem. (2014). *Amanda Hess: "Why Women Aren't Welcome on the Internet"* Mother Jones. 10 January 2014. Accessed 22 May 2015. http://www.motherjones.com/mixed-media/2014/01/amanda-hess-why-women-arent-welcome-Internet
- Rifkin, Jeremy. (). p.260
- Smith, Peter K & Steffgen Georges (Eds.) (2014). Cyberbullying through the new media: Findings from an international network. Florence, KY: Psychology Press, 2014.
- Spears et al. (2013). "Positive uses of new technologies in relationships in educational settings", in "Cyberbullying through the New Media" eds: Smith, Peter and Georges Steffgen. Psychology Press, p. 212.
- Spence, Jessica and Steph Guthrie. (2013) "The 7 Deadly Myths of Online Violence Against Women." Women in Toronto Politics. Posted 11 October 2013. http://witopoli.com/2013/10/11/the-7-deadly-myths-of-online-violence-against-women/
- Storify. Website. Accessed 30 April 2015. https://storify.com/
- Review and appraisal of the implementation of the Beijing Declaration and Platform for Action and the outcomes of the twenty-third special session of the General Assembly. Report of the Secretary General. 15 December 2014. E/CN.6/2015/3

- UNIFEM. (2003). Not A Minute More: Ending Violence Against Women. Ed: Gloria Jacobs. New York. http://iknowpolitics.org/sites/default/files/notminutemore_completebook.pdf
- UN Women (2015) Gender Equality and ICT: In Brief, www.empowerwomen.org/ict4d
- UN Women (2014) Technology and Violence Against Women Framework, www.empowerwomen.org/ict4d
- UN Women (2015) Mapping Access to and use of Mobile Phones to Document, Prevent and Respond to Sexual Violence against Women and Girls in Urban Public Spaces: Findings from 3 Qualitative Methods Studies in the Low-income Communities in the Cities of Marrakech, New Delhi and Rio-de-Janeiro, www.empowerwomen.org/ict4d
- UN Women and Intel (2013) Thought Leadership study on Women and the Web - study done by Dalberg and GlobeScan:
- http://www.globescan.com/news-and-analysis/press-releases/press-releases-2013/98-press-releases-2013/255-intel-announces-groundbreaking-women-and-the-web-report.html
- VAW Learning Network. (2013). Technology-Related Violence Against Women. Issue 4, April 2013. Western University. http://vawlearningnetwork.ca/sites/learningtoendabuse.ca.vawlearningnetwork/files/LN_Newsletter_Issue_4_2013_Online.pdf
- Viswanath, Kalpana. (2015). Creating Engagement in Public Spaces for Safer Cities for Women. UN Habitat. Accessed 12 May 2015. http://unhabitat.org/public-spaces-for-safer-cities-for-women/
- Water Aid Thought Leadership on Access to Water and Violence Against Women. (2012.) Study by GlobeScan. 7 November 2012. http://www.globescan.com/component/edocman/?view=document&id=45&Itemid=0
- West, Jessica. (2014).
- http://www.bwss.org/wp-content/uploads/2014/05/CyberVAWReportJessicaWest.pdf
- Women's Legal and Human Rights Bureau. (2014). "From impunity to justice: Domestic legal remedies for cases of technology-related violence against women" Ed. Richa Kaul Padte. http://www.genderit.org/sites/default/upload/impunity_womens_legal_dig.pdf
- Zadrozny Peter and Raghu Kodali. (2013)Big Data Analytics Using Splunk: Deriving Operational Intelligence from
- Social Media, Machine Data, Existing Data Warehouses, and Other Real-Time Streaming Sources. Apress.

END NOTES

1 Please see http://www.who.int/mediacentre/factsheets/fs239/en/, http://www.un.org/en/women/endviolence/index.shtml and http://www.un.org/en/women/endviolence/factsheets.shtml

2 Please see in particular the various reports of the Broadband Commission at http://www.broadbandcommission.org/resources/Pages/default.aspx

3 Doxing is the Internet-based practice of researching and broadcasting personally identifiable information about an individual.

4 http://www.huffingtonpost.com/2015/05/13/being-a-woman-online-really-sucks_n_7265418.html?ncid=fcbklnkushpmg00000063

5 http://www.telegraph.co.uk/news/uknews/crime/11127808/Twitter-troll-jailed-for-campaign-of-hatred-against-Stella-Creasy.html

6 A San Diego man who operated a 'revenge porn' website and then charged victims to remove nude images and their personal information was sentenced Friday to 18 years in state prison. Kevin Bollaert, 28, was convicted in February of 21 counts of identity theft and six counts of extortion in San Diego Superior Court for running a pair of websites that capitalized on the Internet as a forum for public shaming. The landmark case was the first time a person had been tried for a running revenge porn ring in the United States. Jilted lovers and hackers could anonymously post nude photos of people without their consent, along with personal information about them, at a website Bollaert created and moderated, called ugotposted.com. More than 10,000 images, mainly of women, were posted between December 2012 and September 2013.

7 http://www.unwomen.org/en/what-we-do/ending-violence-against-women/facts-and-figures

8 http://www.unwomen.org/en/what-we-do/ending-violence-against-women/facts-and-figures

9 http://www.unwomen.org/en/what-we-do/ending-violence-against-women/facts-and-figures

10 http://www.Internetworldstats.com/stats.htm

11 Bridging the Gender Gap: Women's Mobile Access and Usage in Low and Middle Income Countries , GSMA, 2015

12 http://www.washingtonpost.com/opinions/online-feminists-increasingly-ask-are-the-psychic-costs-too-much-to-bear/2015/02/19/3dc4ca6c-b7dd-11e4-a200-c008a01a6692_story.html

13 http://www.ohchr.org/Documents/Issues/Opinion/Communications/InternetPrinciplesAndRightsCoalition.pdf

14 Please see in particular the previous reports of the Broadband Commission Working Group on Gender at http://www.broadbandcommission.org/workinggroups/Pages/bbandgender.aspx

15 Jeremy Rifkin, p.260

16 Femicide is generally defined as the murder of women because they are women, though some definitions include any murders of women or girls. Femicide has been used to describe killings of women by intimate partners and family members; it has also been used to describe gender related killings in the community. The term femicide was introduced in the last century to describe killings of women that were gender related in order to recognise the impact of inequality and discrimination, identified internationally as a root cause of violence against women. http://www.womensaid.org.uk/page.asp?section=00010001001400130010&sectionTitle=Femicide+Census (accessed 05.04.15)

17 http://womensenews.org/story/war/110619/gadhafi-said-order-forces-rape-villagers

18 Citron p.253

19 https://ucollege.wustl.edu/files/ucollege/imce/iap.kabance.drp_.pdf

20 http://www.broadbandcommission.org/documents/working-groups/bb-wg-taskforce-report.pdf

21 http://now.avg.com/the-social-Internet-of-things/

22 Bridges, A., & Wosnitzer, R. (2007). Aggression and sexual behavior in best-selling pornography: A content analysis update. International Communication Association. (via http://stoppornculture.org/about/about-the-issue/facts-and-figures-2/)

23 http://stoppornculture.org/about/about-the-issue/facts-and-figures-2/

24 Source: http://www.endvawnow.org/en/articles/300-causes-protective-and-risk-factors-.html?next=301

25 Child sex offenders have been using computers since 1982 in the USA and 1985 in the UK to communicate with and send images to one another, the first person convicted in the UK for possession of indecent images of children was convicted in 1995 (Critically Evaluating Typologies of Internet Sex Offenders: A Psychological Perspective Journal of Forensic Psychology Practice Volume 11, Issue 5, 2011).

26 The Internet has also become the primary means used by international child pornography rings to disseminate their material worldwide. International child pornography rings are operating in dozens of countries, peddling their illicit wares through the Internet and other global distribution networks. Modern technology allows these child pornographers to store vast quantities of digital images on small portable computers easily smuggled into the United States and elsewhere. http://fas.org/irp/threat/pub45270chap2.html#18

27 Kovacs et al. “Don’t let it stand” p.4

28 http://www.nytimes.com/2015/05/10/opinion/sunday/nicholas-kristof-despite-dna-the-rapist-got-away.html?emc=eta1&_r=0

29 http://fra.europa.eu/sites/default/files/fra-2014-vaw-survey-main-results-apr14_en.pdf

30 http://www.unwomen.org/~/media/headquarters/attachments/sections/library/publications/2012/9/csw57-egm-prevention-background-paper.pdf

31 http://www.europe.undp.org/content/geneva/en/home/presscenter/pressreleases/2014/12/10/new-study-highlights-need-to-scale-up-violence-prevention-efforts-globally.html

32 http://www.Internetlivestats.com/Internet-users/

33 http://www.emarketer.com/Article/Smartphone-Users-Worldwide-Will-Total-175-Billion-2014/1010536

34 http://www.cbc.ca/newsblogs/yourcommunity/2014/10/women-talking-video-games.html

35 http://www.theguardian.com/commentisfree/2014/sep/18/52-percent-people-playing-games-women-industry-doesnt-know

36 http://www.pewInternet.org/fact-sheets/social-networking-fact-sheet/

37 http://www.statista.com/statistics/264810/number-of-monthly-active-facebook-users-worldwide/

38 Rifkin, p201.

39 Zadrozny. P.3

40 Rifkin. p 201

41 http://gadgets.ndtv.com/apps/news/whatsapp-claims-over-500-million-active-users-india-the-largest-market-512511

42 www.statistica.com

43 http://www.slate.com/blogs/xx_factor/2014/10/22/pew_online_harassment_study_men_are_called_names_women_are_stalked_and_sexually.html

44 https://globalvoicesonline.org/2014/03/10/european-union-publishes-comprehensive-survey-of-violence-against-women/

45 http://www.ipsnews.net/2014/01/cyber-bullies-target-kenyas-women/

46 Halder & Jaishankar, 2010.

47 http://www5.apc.org/en/system/files/APCWNSP_MDG3advocacypaper_full_2011_EN_0.pdf

48 http://www.un.org/womenwatch/daw/vaw/v-overview.htm

49 Case of Amanda Todd: a 15 year old girl who committed suicide following bullying by a predator who distributed topless images of her from a webcam interaction.

50 VAW Learning Network. (2013) http://www.learningtoendabuse.ca/sites/default/files/Baker_Campbell_Barreto_Categories_Technology-Related_VAW_.pdf

51 The APC challenges the term "revenge porn" as 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. http://www.genderit.org/node/4222

52 West, Jessica (2014) http://www.bwss.org/wp-content/uploads/2014/05/CyberVAWReportJessicaWest.pdf

53 Hughes, Donna M. (2002)

54 http://cyber.law.harvard.edu/vaw02/mod3-2a.htm#ftnt12

55 http://www.cnn.com/2014/02/28/world/asia/china-online-baby-trafficking-crackdown/

56 Voices from Digital Spaces: Technology Related Violence against Women (2011, p. 26 & 27)

57 http://www.genderit.org/sites/default/upload/case_studies_rdc2_1.pdf

58 http://www.genderit.org/sites/default/upload/case_studies_col4_1.pdf

59 http://www.genderit.org/sites/default/upload/case_studies_byh1_1.pdf

60 https://www.apc.org/en/pubs/cases-women%E2%80%99s-experiences-technology-related-vaw-a

61 Rifkin p.258

62 http://www.canadianwomen.org/facts-about-violence

63 http://www.canadianwomen.org/facts-about-violence

64 http://www.comminit.com/communicating_children/content/voices-against-violence-non-formal-education-

programme-children-and-youth-help-stop-viol

65 http://www.un.org/en/women/endviolence/orangeday.shtml

66 https://www.kickstarter.com/projects/4096561/heartmob/description).

67 Smith & Steffgen Cyberbullying through the New Media p. 85

68 See (http://sites.google.com/site/costis0801/)

69 https://www.takebackthetech.net/mapit/reports/view/552

70 Citron. P.229

71 http://www.theguardian.com/technology/2013/may/29/facebook-campaign-violence-against-women accessed 27.04.15

72

73 http://www.intel.com/content/dam/www/public/us/en/documents/pdf/women-and-the-web.pdf

74 http://www.un.org/womenwatch/daw/vawg/handbook/Handbook%20for%20legislation%20on%20violence%20against%20women.pdf

75

76 Raja, 2014

77 Hess, 2014

78 http://www.genderit.org/sites/default/upload/flow_corporate_policies_formatted_final.pdf

79 http://www2.ohchr.org/english/bodies/hrcouncil/docs/17session/A.HRC.17.27_en.pdf

80 Kavita Dogra, We Talk Women, Canada. Interview notes March 31st 2015

81 Citron (p. 231)

82 http://www.theguardian.com/technology/2015/apr/21/twitter-filter-notifications-for-all-accounts-abuse

83 Halter 2015

84 http://www.consumerreports.org/cro/magazine/2012/06/facebook-your-privacy/index.htm

85 http://www.theguardian.com/technology/2014/jun/03/facebook-children-join-social-network

86 Smith & Steffgen p.87

87 http://www.genderit.org/sites/default/upload/flow_corporate_policies_formatted_final.pdf

88 http://cyber.law.harvard.edu/sites/cyber.law.harvard.edu/files/Final_Report_on_Account_Deactivation_and_Content_Removal.pdf

89 http://www.polygon.com/2014/11/14/7219451/sweden-wants-to-label-games-that-promote-gender-equality

90 http://articles.economictimes.indiatimes.com/2013-09-14/news/42062523_1_device-amrita-university-communication

Cyber security device to protect women from violence

91 Viswanath, Kalpana and Ashish Basu. (2015).

92 http://www.gsma.com/connectedwomen/kenya-and-the-rise-of-the-call-blocking-app/

93 See http://www.cisco.com/web/IN/cwdf14/index.html#~CMARC

94 https://www.apc.org/en/news/section-j-footnotes-headlines

95 APC VAW Online Infograhic

96 http://thewebindex.org/report/#4.2_gender-based_violence_online

97 http://thewebindex.org/report/#1._executive_summary:_the_web_and_growing_global_inequality

98 http://witopoli.com/2013/10/11/the-7-deadly-myths-of-online-violence-against-women/

99 The Digital Millennium Copyright Act (DMCA) contains two main sections that have been a source of particular controversy since they went into effect in 2000. The “anti-circumvention” and the”safe harbor” provisions. EFF has fought hard against the DMCA circumvention provisions in the courts, Congress and other forums, and has fought equally hard to make sure the DMCA safe harbors shelter innovation and creativity.

100 An Exploratory Study of Women and Verbal Online Abuse in India By Anja Kovacs Richa Kaul Padte Shobha SV Internet Democracy Project New Delhi, April 2013

101 http://www.genderit.org/sites/default/upload/flow-cnyst-summary-formatted.pdf

102 http://www.genderit.org/sites/default/upload/flow-cnyst-summary-formatted.pdf

103 http://www.nowldef.org/history-vawga#sthash.sWCnxx8m.dpuf

104 Citron; p.149

105 Citron; p. 152

106 http://Internetdemocracy.in/reports/keeping-women-safe-gender-online-harassment-and-indian-law/

107 http://www.cybervictims.org/CCVCresearchreport2015.pdf

108 Citron, p. 168

109 Broadband Commission Gender Working Group (2014) Draft Analysis: Gender and ICT Policy Workstream

110 https://www.apc.org/en/node/8041/

111 http://www.genderit.org/sites/default/upload/domestic_legal_remedies_for_technology-related_violence_against_women_review_of_related_studies_and_literature.pdf

112 Athar, 2015

113 (http://www.intgovforum.org/cms/best-practice-forums) Best practices forums are one of the intersessional activities and its idea is for experts from government, business, civil society and the academic and technical communities to work through mailing lists and online virtual meetings to come up with best practices on selected themes.

114 See for example https://www.unsceb.org/tags-ict/cybersecuritycybercrime and http://www.unsceb.org/CEBPublicFiles/Chief%20Executives%20Board%20for%20Coordination/Document/REP_CEB_201311_CEB2013-2.pdf

115 http://www.un.org/apps/news/story.asp?NewsID=50610#.ValXnPlViko

116 http://www.genderit.org/node/4097.

117 UNESCO. (2014). Review and appraisal of the implementation of the Beijing Declaration and Platform for Action and the outcomes of the twenty-third special session of the General Assembly. Report of the Secretary General. 15 December 2014. E/CN.6/2015/3

118 PROGRAMMED TO KILL - Video Games, Drugs, and The 'New Violence' http://www.21stcenturysciencetech.com/articles/New_violence.html

119 Video game use peaks during middle childhood with an average of 65 minutes per day for 8–10 year-olds, and declines to 33 minutes per day for 15–18 year-olds [16]. And most of these games are violent; 94% of games rated (by the video game industry) as appropriate for teens are described as containing violence, and ratings by independent researchers suggest that the real percentage may be even higher Haninger K, Thompson KM. Content and ratings of teen-rated video games. JAMA. 2004;291(7):856–865. http://www.ncbi.nlm.nih.gov/pmc/articles/PMC2704015/#R17

120 Citron, Danielle Keats (2014) Hate Crimes in Cyberspace, Harvard University Press p, 99












2015
Photo credits:Shutterstock

BROADBAND COMMISSION
FOR DIGITAL DEVELOPMENT