Final report of the Broadband Commission Working Group on Gender, September 2015

Combatting Online Violence Against Women & Girls: A Worldwide Wake-up Call

Highlights

- A new report from the United Nations Broadband Commission for Digital Development aims to mobilize the public and private sectors around concrete strategies aimed at stemming a rising tide of online violence against women and girls.

- Violence Against Women and Girls (VAWG) is already a problem of pandemic proportion; research shows that one in three women will experience some form of violence in her lifetime. Now, the new problem of 'cyber VAWG' could significantly increase this staggering number, as **our research suggests that 73% of women have already been exposed to or have experienced some form of online violence**. With social networks still in their relative infancy, this is a problem that urgently needs to be addressed if the Net is to remain an open and empowering space for all.

- **The sheer volume of cyber VAWG has severe social and economic implications for women's status on the Internet.** Threats of rape, death, and stalking put a premium on women's emotional bandwidth, take-up time and financial resources including legal fees, online protection services, and missed wages. **Cyber VAWG can have a profoundly chilling effect on free speech and advocacy.**

- **Women aged 18 to 24 are at a heightened risk of being exposed to every kind of cyber VAWG**; 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.

- In the EU-28, 18 per cent of women have experienced a form of serious Internet violence at ages as young as 15. This corresponds to about 9 million women.

- **Complacency and failure to address and solve cyber VAWG could significantly impede the uptake of broadband by women everywhere**; without action, an unprecedented surge of 21st century violence could run rampant if steps are not urgently taken to rein in the forms of online violence that are escalating unchecked.

The scope of the cyber VAWG problem

- Violent online behaviour ranges from online harassment and public shaming to the desire to inflict physical harm including sexual assaults, murders and induced suicides. With the proliferation of the Internet, online violence against women has taken on a global dimension. **Online crimes are not a 'first world' problem; they seamlessly follow the spread of the Internet.**

- 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. In the age of the social Internet, networks of networks of 'distributed intelligence' and accessible mobile platforms are reaching ever more remote corners of the world. **Mobile Internet access means that these can come at any time, and can follow their targets everywhere.**

Most cyber VAWG goes unreported

- The WWW Foundation has found that **law enforcement agencies and the courts are failing to take appropriate actions for cyber VAWG in 74% of 86 countries surveyed**.

- One in five female Internet users live in countries where harassment and abuse of women online is extremely unlikely to be punished (source: The Web Index).

- One example from around the world: A report from India suggests that only 35% of women in that country have reported their victimization… women often prefer not to report cyber VAWG for fear of social repercussions.

- The rapid spread of the Internet means that at a national level effective legal and social controls of online anti-social and criminal behaviours continue to be an immense challenge. **Rigorous oversight and enforcement of rules banning cyber VAWG on the Internet is going to be an essential foundation stone if the Internet 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 recognize and act on the basic principle **that an unsafe Internet will mean that women will frequent the Internet less freely, with costly societal and economic implications**.

Industry safeguard protocols

- **Industry players are important digital gatekeepers**. They include ISPs, mobile phone companies, social networking sites, online dating and gaming sites, website operators and software developers.

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

  - Better systems for cooperating with law enforcement
  - More effective takedown procedures for abusive and harmful content
  - A possibility of account termination for misconduct
  - Production of transparency reports of records specific to cyber VAWG, detailing how and when they have responded.

Key Recommendations of the Report

Best practice should be based on **3 'S's – Sensitization, Safeguards and Sanctions**

- Preventative measures through **public sensitization**. Changing social attitudes and norms is the first step to shifting the way online abuse is understood and the seriousness with which it is treated. There is a need for public education and education of enforcement agency staff, such as police.

- Promotion of **safeguards** for online safety and equality on the Internet for women and girls. Traditional Violence Against Women safety frameworks include women's shelters, crisis centres, help lines and education: **The digital world also requires safety measures to keep up with a rapidly evolving Internet.** This will necessarily require resources, attention and active participation of digital gatekeepers in industry, civil society and governments.

- Putting in place and enforcement of **sanctions** through courts and legal systems to define and enforce compliance and effective punitive consequences for perpetrators.

- Each of these pillars of **sensitization**, **safeguards** and **sanctions** supports the other pillars, and will need consistent, collaborative action at many levels.

Prevent cyber VAWG through changes in social attitudes

Sensitization

Society to prevent all forms of cyber VAWG through training, learning, campaigning, and community development

Justice and security/police to integrate cyber VAWG concerns into all criminal and cyber-security training

Oversight & monitoring to minimize risks for women & girls

Safeguards

Industry to maintain responsible Internet infrastructure & customer care practices

Development of technical solutions

Promote due diligence & duty to report abuse

Adapt & apply laws & regulations

Sanctions

Develop laws, regulations and governance mechanisms

Courts and legal systems to enforce compliance and effective punitive consequences for perpetrators

Consultations on a cyber civil rights agenda